IDA

INSTITUTE FOR DEFENSE ANALYSES

Information Operations: A Research Aid

Includes Coverage of: Information Warfare, Information Assurance, and Infrastructure Protection

J. V. Gray, Principal Investigator

September 1997

IDA Document D-2082

Log: H 97-002837

This work was conducted under IDA's central research program. The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

INSTITUTE FOR DEFENSE ANALYSES

IDA Document D-2082

Information Operations: A Research Aid

Includes Coverage of: Information Warfare, Information Assurance, and Infrastructure Protection

J. V. Gray, Principal Investigator
W. J. Barlow
J. W. Barnett
J. L. Gerrity
R. D. Turner

PREFACE

This document, funded as an IDA Central Research Project, has been prepared to examine the concepts and elements of "Information Operations" (IO) to create a useful and coherent research aid both within IDA and ultimately by persons outside the Institute. A recent DoD Directive (S-3600.1) formally established IO as the overarching concept that includes, such functions as Information Assurance, Information Warfare, and Information Superiority under its umbrella. The subject of national Infrastructure Protection, though not explicitly covered in the directive, is by reasonable extrapolation an included topic. This document provides an annotated bibliography of selected written sources, identifies principal categories and main themes, and reports the results of interviews with selected leading thinkers in this topic area. As such, the document is an ideal starting point for researchers desiring to quickly know the basic facts about these subjects.

The principal investigator was Miss Jaime Gray from the University of Virginia who served as a summer intern at IDA in 1997. She prepared the bibliography, conducted the interviews, and suggested the main themes. She was assisted at a modest level of support by the other co-authors. All the co-authors are indebted to a review committee of Dr. David L. Randall, Dr. John R. Shea, RADM Grant A. Sharp (USN, Retired), and Mr. Philip J. Walsh for their helpful suggestions and insights.

(This page is intentionally blank.)

CONTENTS

Part 1—Summary

Part 2—Discussion

Appendixes

LIST OF FIGURES

LIST OF TABLES

(This page is intentionally blank.)

Part 1

SUMMARY

SUMMARY

Purpose

The purpose of this paper is to provide an aid to researchers in identifying issues and associated documentation concerning Information Operations, Information Warfare, and related elements including Information Assurance and Infrastructure Protection.

Background

Since the promulgation of DoD Directive TS-3600.1, *Information Warfare (IW)*, in December 1992, the Joint Staff, the Services, defense agencies, and the intelligence community have initiated a large number of implementing activities. The Directive viewed IW as an integrating strategy encompassing a broad array of disciplines including command, control, communications, and computers (C4), command and control warfare (C2W), C3 countermeasures (C3CM), information systems security (INFOSEC) and intelligence support. C2W and C3CM were already formally established by Joint Chiefs of Staff (JCS) Directives as the integrating strategies for the use of military electronic warfare, deception, operations security, psychological operations, and the physical destruction of enemy C3 targets (and for the protection of U.S. C3 assets against such attacks). The DoD Directive also recognized INFOSEC is a major new discipline that has emerged as a consequence of the integration of computer systems security (COMPUSEC) and communications security (COMSEC) disciplines.

The foregoing Directive was canceled and replaced by DoD Directive S-3600.1 on December 9, 1996. The new Directive was titled *Information Operations (IO)* and set forth a host of new terms and concepts included under the IO umbrella. As a consequence, there is a scramble of new activity by DoD organizations, industry, and academia to match past and current work to be consistent with the new taxonomy of terms and functions. Researchers new to the subject area will face a bewildering assortment of differing uses of the same terms.

This Document

To help alleviate this situation, IDA undertook to provide a research aid document that:

- Suggested a range of subject areas relevant to Information Operations
- Prepared an annotated bibliography of research materials (arranged by principal subject areas) believed to be of most value to new analysts of this field
- Reported the results of interviews with several recognized experts to include the identification of main themes and suggested improvements.

The chosen range of principal subject areas for preparation of the bibliography is shown in Table 1. All the materials examined were listed under one or more of the 10 major categories, along with a brief annotative description.

Table 1. Bibliographic Information Categories

Information Operations
Defensive Information Operations
· Information Assurance
· Information Protection
Information System
Information Warfare
National Policy
Technology
Perspectives
Reference Material

Main Themes

Some of the main themes and principal points that emerged from the interviews included the following subset of comments:

- There is a lack of a coherent national policy on these topics.
- There is an absence of common, agreed terminology.
- Many institutions have failed to understand the problems and hence have not adopted appropriate roles and responsibilities.
- Significant issues are not being adequately addressed.
- Vulnerabilities need to be analyzed.

- The military has a good start, but has a long way to go.
- The Civil Sector is hardly aware of the need for information security, doesn't understand the need, and won't invest in a solution.
- A National Center is needed for information protection to assist cooperative public-private efforts such as indications, warning, and response to attacks.
- The United States should develop and harden a minimum essential infrastructure.

Scope

The paper provides an overview of Information Operations and Information Warfare, a series of interviews of selected experts in the field, and an annotated bibliography of associated documentation. The overview (Chapter I) provides a framework for examining Information Operations and Information Warfare based on terminology and included concepts established in or derived from current national and defense policy guidance and practices. The interviews (Chapter II) establish principal themes pursued by the interviewees. Those themes provide a basis for identifying issues for study and analysis. The annotated bibliography (Chapter III) facilitates insight into the significant array of pertinent documentary material and identification of items of potential interest to the researcher. Appendixes provide a glossary of terminology and definitions and the text of actual interviews.

(This page is intentionally blank.)

Part 2

DISCUSSION

I. OVERVIEW

This overview presents a framework for examining Information Operations and Information Warfare. It is derived from current U.S. Government activities, which treat aspects of the subject, principally the policies and doctrine set forth in the Department of Defense (DoD). The framework is used subsequently herein to organize related themes found in interviews of experts in this field and the bibliography of Government documentation and related publications.

A. BACKGROUND

The DoD has been striving since the late 1970s to codify as an integrated strategy the military concept of countering an adversary's information system while protecting one's own information system. Although this concept has been applied in various ways throughout the history of warfare, the effort to pursue it by integrating the use and protection of the powerful means available in the dawning information age was initiated by DoD directive in 1979.[1] Over the intervening years, the terminology and associated definitions have changed as related concepts have matured and with recognition of the dawning of the information age and the associated Resolution in Military Affairs. During this period, too, terminology became as much a divisive issue as one fostering unity of thought and purpose wherein the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff (JCS) and the Joint Staff, and the Services adopted an array of differing terms and definitions. There now appears, however, to be substantial movement within DoD toward common terminology and definitions. In particular, such movement is seen in adoption by the Chairman of the Joint Chiefs of Staff and the Joint Staff of terminology recently promulgated by OSD. Such agreement may, in turn, lead to greater doctrinal consistency among the Services.

Although DoD and JCS have thus been dealing with information warfare as an integrated strategy for 2 decades, there has been no similar action to adopt a codified

---

1 DoD Directive 4600.4, "Command, Control and Communication (C^3) Countermeasures," August 27, 1979. (Subsequently superseded and canceled.)

approach for integrating the information activities of the various departments and agencies of the U.S. Government as it deals with adversary nations and other threats to national security. There has been, nevertheless, recent recognition of the threat to the national information infrastructure and of the need for concerted Government action in coordination with key elements of the civil sector. The President's National Security Strategy of February 1996 put the matter in this way:

> The threat of intrusion to our military and commercial information systems poses a significant risk to national security and is being addressed.

When addressing the overall concept of countering an adversary's information and information system while protecting one's own, much of the literature, official and otherwise, has used the term Information Warfare (IW). As will be developed further below, an overarching term, Information Operations (IO), has been adopted recently in DoD policy to replace the former umbrella term (IW). Specifically, IO is defined as:

> Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also known as IO.

The term "Information Warfare" is retained but with the more restricted definition:

> Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW.

B. FRAMEWORK FOR INFORMATION OPERATIONS AND INFORMATION WARFARE

The framework for IO and IW reflects current activities to implement those concepts at the national level and within the DoD. As noted in the background, above, national level attention has focused on protection of the national information infrastructure. Although such focus is of limited utility in providing an overall framework, a summary of related activities provides context for associated documentation and publications. In contrast, implementation within DoD permits derivation of a framework for IO and IW in the form of functional hierarchies stemming respectively from the broad concepts embodied in the definitions of those terms.

1. Implementation At National Level

In response to the need to address the threat to our military and commercial information systems, the President, by Executive Order 13010 dated 15 July 1996, created a Commission on Critical Infrastructure Protection. The commission has been charged with addressing what Government and industry must do to protect key infrastructure from physical or cyber attacks as well as natural disasters. The eight national key infrastructures of concern named in the Executive Order are listed in Table 2.

Table 2. Key Infrastructures

Telecommunications
Electricity
Banking and Financial Services
Gas and Oil Production and Delivery
Transportation
Water Supply
Government Continuity of Services
Emergency Services (Medical, Fire, etc.)

Findings of this Commission are due to be presented in October 1997.

In addition, the President, by the same Executive Order on July 15, 1996, created an Infrastructure Protection Task Force (IPTF) mandating that Government and industry cooperate to develop a strategy for ensuring continued National Information Infrastructure (NII) protection. That task force is to function indefinitely and will be instrumental in implementing the findings of the aforementioned presidential commission. Thus, although not achieving codification of a broad all-encompassing information strategy (offensive as well as defensive), significant steps have been taken on the defensive side.

2. Implementation in DoD

Department of Defense Directive S-3600.1, *Information Operations*, December 9, 1996, sets forth relevant policy and a host of new information terms and concepts. Subsequent development of implementing policy and doctrine by the Joint Staff expands on the DoD concepts by identifying supporting or constituent elements with more new terminology and definitions. Coupled with pertinent existing concepts and terminology, the new set of terms and included concepts provides a basis for portraying IO and IW as functional hierarchies. Those terms and their definitions are included in Appendix A.

Figure 1 portrays a suggested hierarchy for IO. Two main aspects, Defensive IO and Offensive IO, each in turn involve a series of elements or activities, some of which have roles in both Defensive and Offensive IO. The operations are founded on the information system, an array of military capabilities, and intelligence support.

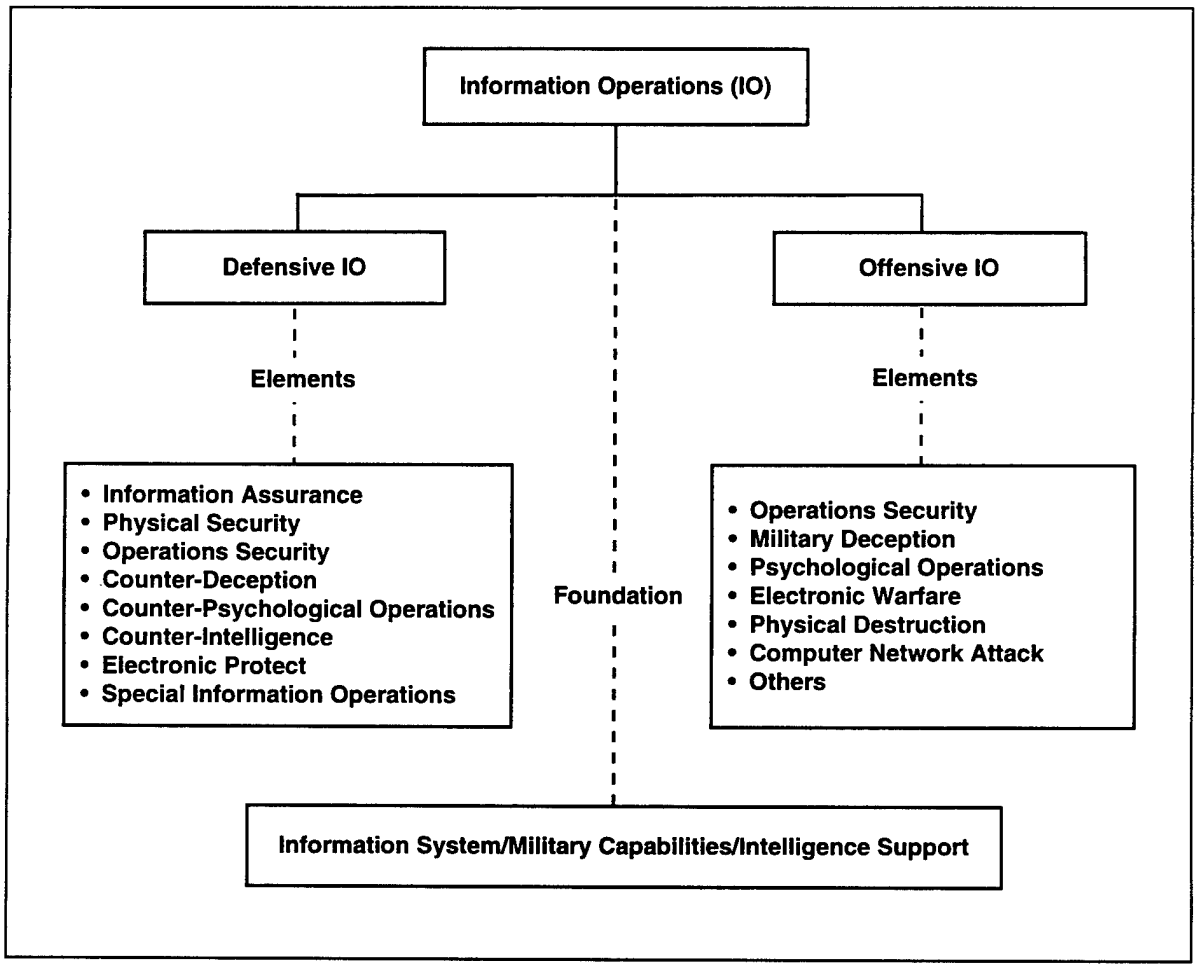


Figure 1. Information Operations Hierarchy

The first element listed under Defensive IO, Information Assurance, is a relatively new term in military lexicon; its concept and scope are, therefore, elaborated. Information Assurance is defined in the DoD Directive in Appendix A as:

> Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Objectives established in this definition have been clarified as presented in Table 3.[2]

Table 3. Objectives of Information Assurance

Term	Definition
Availability	Assured access by authorized users
Integrity	Protection from unauthorized change
Authentication	Verification of originator
Confidentiality	Protection from unauthorized disclosure
Nonrepudiation	Undeniable proof of participation

The growing range of threats to the information environment, including the National Information Infrastructure and the Defense Information Infrastructure, has raised this element of IO to an item of congressional interest and to the forefront of DoD activities. Those threats include hackers, insiders and authorized users, criminals and organized crime, terrorists, industrial and economic espionage, and foreign countries. The process for implementing Information Assurance, a facet of Defensive IO, follows the model shown in Figure 2 which is applicable during peace, crisis, and war, and across the range of military operations.[3]

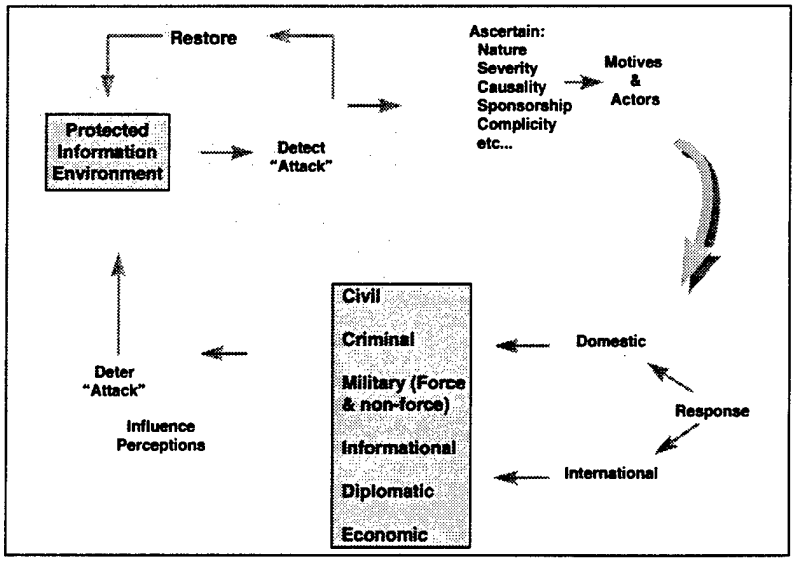


Figure 2. Defensive IO Implementation Model

---

2 Table 3 is derived from a Joint Staff pamphlet, titled "Information Warfare," undated.

3 Figure 2 is extracted from CJCSI 6510.01 B, 22 August 1997.

Figure 3 portrays a hierarchy for Information Warfare. This framework extends beyond that derived from DoD terminology by portraying the domestic and diplomatic IO activities inherent in situations of crisis and war. Those activities are shown as "implied" because, although historically and increasingly employed, as discussed above, no codified concept for their implementation along with military IO activities as an integrated national level strategy. Military IO activities are shown to include Command and Control Warfare (C2W) and other target sets with vulnerable information components. C2W is a subset of information operations in military operations focusing in countering adversary command and control capabilities while protecting friendly command and control capabilities. (C2W is defined in Appendix A.) Other target sets are shown to reflect possibilities such as military attack of information systems beyond the target set of adversary command and control capabilities but of military significance.

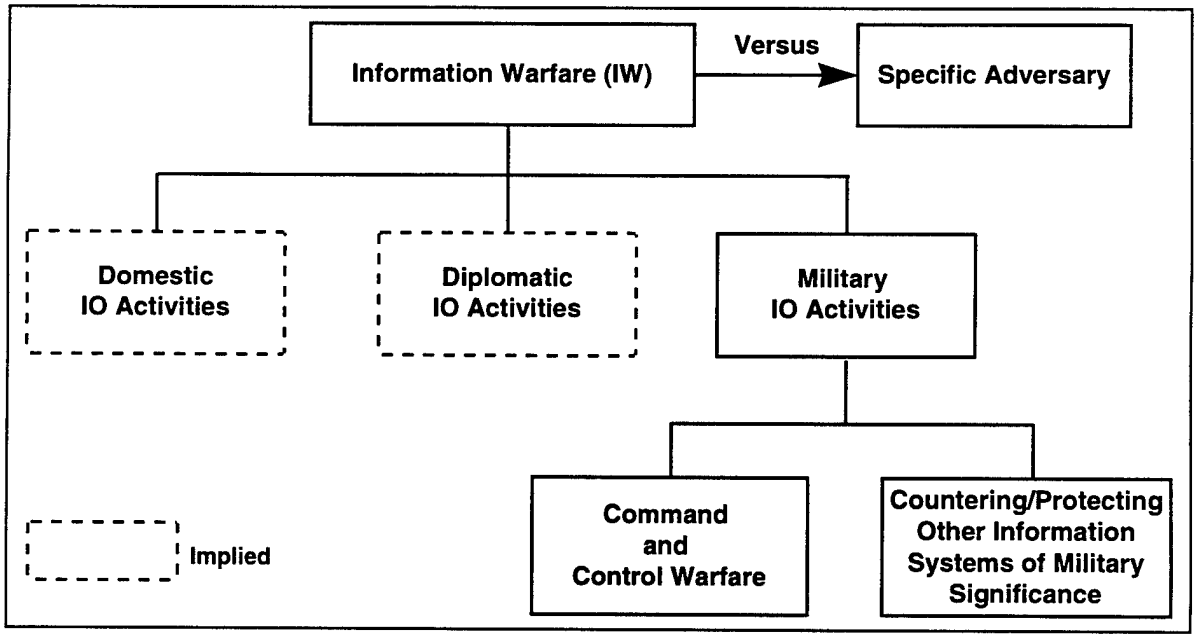
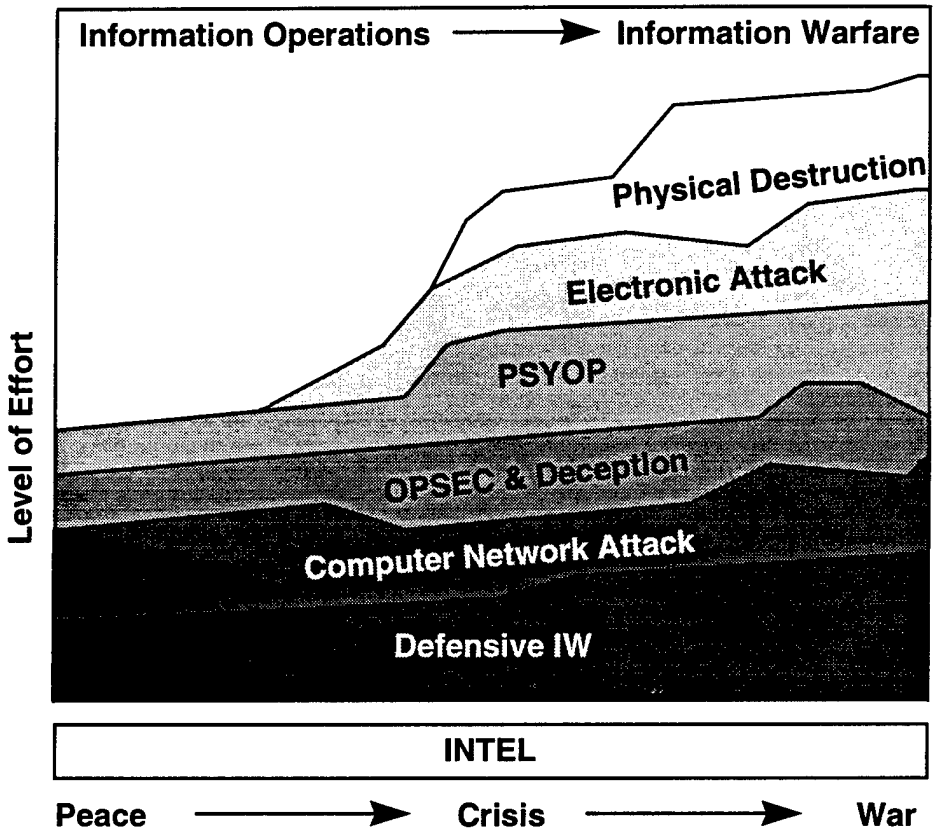


Figure 3. Information Warfare Hierarchy

The timing and relative level of effort associated with IO and IW are shown in Figure 4. Effort associated with Defensive IO and aspects of selected subelements are continuous in peace and intensify in times of crisis and war. Offensive IO activities such as electronic attack and physical destruction are to be undertaken as crisis escalates to war.



Source: Derived from a Joint Staff pamphlet, titled, "Information Warfare," undated.

Figure 4. Illustrative Engagement Sequence

(This page is intentionally blank.)

II. INTERVIEWS

The opportunity arose to interview some recognized national figures on various aspects of Information Operations. We undertook to prepare a set of questions designed to evoke comments on key issues and suggest solutions to well-known problems. Set forth below are the names and positions of the interviewees, the specific questions asked, the main points and themes expressed; a write-up of the substance of the complete interviews is set forth in Appendix B.

A. INTERVIEWEES

The following individuals were chosen for interview based on their demonstrated knowledge of the area (e.g., author, academic, Government official) and availability within the Washington area to participate in the study effort:

- *Kenneth C. Allard*
  - Adjunct Professor in National Security Studies at Georgetown University
  - Former Dean of Students, National War College
  - Former Congressional Fellowship, Assistant to Senator John Warner
  - Frequent lecturer and guest commentator for TV networks on Information Operations and Information Warfare
  - Author of Command, Control and the Common Defense, an award-winning book.
- *Alan D. Campen*
  - Contributing Editor *SIGNAL* magazine
  - Manager AFCEA International Press
  - Adjunct Professor, School of Information Warfare and Strategy, National Defense University (NDU)
  - Author and lecturer on Information Warfare.

- *James R. Gray*
  - Colonel, USAF (Ret.)
  - Extensive Joint service in the field of IO/IW
  - Staff, Avenue Technologies, Inc., currently investigating issues related to national infrastructure protection.
- *Daniel T. Kuehl*
  - School of Information Warfare and Strategy, National Defense University
  - Course Director, Information Strategies Program
  - Former member of "CHECKMATE," planning team developing the air campaign plan used in Desert Storm
  - Has authored work on "Cyberwar: Security, strategy and Conflict in the Information Age" (for AFCEA)
- *John E. McClug*
  - Supervisory Special Agent, Federal Bureau of Investigation (FBI)
  - Member of the Infrastructure Protection Task Force created by Executive Order 13010
  - Unit Chief in FBI Computer Investigation and Infrastructure Threat Assessment Center (CITAC).
- *Melissa McPherson*
  - Staff, Rand Corporation, Santa Monica, CA
  - Extensive research and analysis in field of IO/IW
  - Author and lecturer on Information Age Warfare.
- *Winn Schwartau*
  - President of Interpact, Inc.
  - Author of *The Basics of Information Warfare*, presented at INFOWARCON, 1997.
  - Team Leader, Manhattan Cyber Project, Information Warfare and Electronic Civil Defense
  - Author of *Information Warfare: Chaos on the Electronic Superhighway* and its 2nd edition, *Cyberterrorism: Protecting Your Personal Security in the Electronic Age*

- *Howard C. Whetzel*
  - President, Avenue Technologies, Inc., currently investigating issues related to national infrastructure protection and applications of advanced technologies to intelligence and Information Operations activities.
  - Extensive experience in fields of national and theater intelligence and electronic warfare
  - Former Assistant to the Director, Defense Intelligence Agency (DIA) for Electronic Warfare and Joint C3I Systems
  - Developed Vulnerability Analysis on U.S. C3I Systems
  - Author of "Responding to the Threat: U.S. C3I Joint REC and ECCM."

B. INTERVIEW QUESTIONS

The following questions were devised to elicit the views of the interviewees:

1. What do you consider to be the major issues in the broad field of Information Operations/Information Warfare/Information Assurance?
2. Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level?

   By the military?

   In the civil sector?
3. How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention?
4. The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in Government for dealing with this issue at the national level?
5. What obstacles do you see to developing an effective national "cyber defense," and what should be done to overcome them?
6. The "information age" can be seen as a combination of numerous necessary elements, including technology, the human factor, process, and policy. It is vital to our understanding of and response to this new era that we address all necessary changes in both ideology and practice. How should we as a nation focus our resources to address the necessary elements of change and use these elements to our advantage as well as defend ourselves in the information age?

   (Defense seems a monumental task, and is, as such, the subject of the current

President's Commission on Critical Information Infrastructure Protection. The suggestion by the Commission is that the fix to this is obviously a public and private partnership that tackles the issues of information assurance, especially Indications and Warning (called "operational warning" by one of the panels), on a sector-by-sector basis. Each "critical" industry, and subsequent type of information infrastructure, has its own needs and must be addressed within the context of its specific capabilities and vulnerabilities. With that framework in mind, however, what suggestions might be added?)

7. How should we approach the use of IW concepts and strategies with our allies in order to achieve an ordered response to crises?
8. What impact will the evolution of information technologies have on preventing and/or resolving conflicts with non-nation-state actors (e.g., hackers, etc.)?
9. Most importantly, in light of everything that needs to be done, what is your prioritization of actions to respond to the situation? Where should we focus our attention first, and where do we go from there?

C. POINTS MADE AND PRINCIPAL THEMES

An examination of all the interviews disclosed some common beliefs and insights that permeated the subject area. The following items constitute a succinct overview of interviewees' comments. (See Appendix B for detailed interview with each individual.)

1. Major Issues

- There is a universal inability to comprehend the effects of the information age on principal endeavors of mankind.
- Omni-linking of the global electronic digital world is increasing, thereby creating greater risk.
- A coherent national information policy is lacking.
- Institutions have failed to understand and adopt appropriate roles and responsibilities.
- "Public privacy" is not protected.
- There is an absence of common, agreed-on terminology.
- We must realize that the emergence of cyberspace represents an operational environment.
- The IO field must defeat skepticism and win acceptance.

- IO can potentially be both over- and under-emphasized.
- There is the danger that the U.S. military will assume that it can guarantee information dominance on a hostile battlefield.
- We must develop a new understanding of "force" in the information age.
- A generational gap exists between senior leadership and those who understand the current state of technology.
- Differentiation must take place between the two lunatic fringes: "The sky is falling" and "There is nothing new here."
- Responsibility for protection of critical infrastructure should be divided between Government and the private sector.
- There is hostility and a lack of trust in corporate efforts to reduce vulnerabilities to malicious attack.

2. Status of Issues and Suggestions for Addressing:

- Issues are not adequately addressed.
- We need to analyze our vulnerabilities.
- We need to treat information as a national asset.
- Deterrence has been largely ignored.
- Social implications have been ignored.
- The military has good start but has long way to go.
- The military needs to rationalize its organizational structure in light of the information-based environment.
- The military is working the problem, but available funding will go to platforms and weapons, not information security.
- The military is increasingly focused on information warfare instead of information age national security.
- The civil sector is barely aware of information security, doesn't understand it, and won't invest in a solution.
- We need to build understanding through simulations and modeling.
- Until and unless there is some national emergency, nothing will happen.
- Insufficient attention is paid to implications of the offensive side of IW; on the defensive side, we have hardly begun.
- U.S. offensive IO planners should share information with defensive IO planners.

- The Presidential Commission on Critical Infrastructure Protection (PCCIP) is a good start, but some believe it reported little more than was already apparent.

3. Suggestions for Addressing Issues

- The increased use of simulation and modeling will help build a better understanding of information age warfare.
- National policy initiatives for information assurance should be continued and refined.
- A Presidential national policy delineating responsibilities of the various organizations would be helpful.
- A "Center of Excellence" could be created to respond to threats.
- An anonymous reporting mechanism for necessary statistical databases should be fostered.
- It is important that all groups involved recognize that IW is not just about electronics and computers, but it also involves the mind.

4. Governmental Responsibilities for Information Operations

- Presidential leadership is required.
- A national center is needed, run by a department other than DoD, possibly a new department.
- Within DoD, this is a possible new role for the Strategic Command (STRATCOM).
- IO should not be the sole jurisdiction of either the military or domestic law enforcement.
- A single organization that directs a cooperating and integrated effort of a number of relevant agencies is needed.
- Federal Government will not be a major player because it lacks authority and trust.
- The Federal role should be limited to:
  - Focused intelligence and warning
  - Today's law enforcement duties
  - Focused research and development (R&D) on defenses
  - Security standards

  - A nationwide attack, detection, reporting, and security system
  - Education.
- The FBI should be the coordinating agency for cyberwar.

5. Obstacles to National "Cyber Defense" and Proposed Actions

- A national policy is absent.
- Both policy and procedures present impediments.
- The various viewpoints of Government agencies and industry create disparate perceptions of the problem.
- American culture values privacy and freedom of speech.
- The actors/interests are multiple.
- Civil defense must be conceptualized entirely new terms.
- The incentive for investing in security is lacking.
- There is no consensus that a threat or need for corrective action exists.
- The threat and basic aspects of information operations are over-classified.
- Military positions are vulnerable because support mechanisms are unclassified.

6. How To Focus Resources

- For DoD, each Service should be directed to maintain a uniformed capability in IO vice heavy dependence on civilian contractors.
- Identification of vulnerabilities, supervision by a non-DoD department, and education of our leaders is necessary in the civilian sector.
- There is a need to turn to exploiting information technology's capacity for enhancing speed and precision on the battlefield.
- Technology should be leveraged at strategic, operational, and tactical levels simultaneously.

7. Approach to Use with Allies

- This is an international issue, and we must work freely with our allies.
- We must "get our own house in order" before we can work effectively with allies.
- We must work to keep allies informed.
- We should share advances in information security.

- Our three-dimensional society must understand how to cope with the two-dimensional societies of our adversaries.
- Provisions for graceful degradation of information networks are absent.
- The lack of interoperability requires a rigid, inflexible series of standards, commercially based and enforced.
- We need vertical coalition assistance where the United States provides the technology, a large portion of intelligence, and much of the know-how, while less IW-ready allies provide the manpower and firepower.
- Sharing is risky but not as bad as the risk that a trusted insider may become an informant.
- Other nations will or will not cooperate on this as they do or don't on any other security interest.

8. Conflicts with Non-State Actors

- The advent of information warfare makes such conflict more likely.
- Distinguishing between state and non-state actors is increasingly difficult.
- The civilianization of IW and replacement of mass with efficiency as the decisive element in war create a potential for non-state actors to compete viably in global strategic conflict.
- Information power allows speed and precision to override benefits formerly accrued from mass.

9. Priority Actions

- Obtain national leadership.
- Form a clear delineation of responsibilities.
- Establish a national IO center.
- Consider establishing a Department of Information.
- Debate issues of information age, e.g., vulnerability, privacy, and unbridled access.
- Reduce threat classification.
- Embark in a catch-up education program.
- Create a consensus on what IO constitutes.
- Develop and harden a minimum essential infrastructure.

- Continue to develop our own capabilities for leveraging advantages in information technologies.
- Examine effect of potential changes in warfare on society and the international system and examine what these changes mean for the future use of war as an instrument of international politics.
- Improve the security of our national information infrastructure and the tactical military systems that rely on it.
- Reconsider the sphere of classification of military operations, especially the need to include support mechanisms.
- Spur coalescence of the public and private sectors to see this as a shared responsibility.
- Pursue the results of the PCCIP.
- Rationalize the military information systems: how to defend them and how to modernize them.
- Establish criteria for selecting future systems to include interoperability, security, and leveraging availability of advanced commercial technology.

(This page is intentionally blank.)

III. ANNOTATED BIBLIOGRAPHY

The bibliography is organized mainly under key subject areas related to Information Operations as discussed in Chapter II. Specifically, those subject areas are the following:

- Information Operations
- Defensive Information Operations
  - Information Assurance
  - Infrastructure Protection
- Information System
- Information Warfare
- National Policy
- Simulations
- Perspectives
- Technology
- Reference Material.

Several subject areas are related to terms and included concepts in DoD policy and associated joint policy and doctrine as set forth in Appendix A and discussed in Chapter II. In such cases, those terms and their definitions are included with the respective headings in the bibliography that follows:

A. INFORMATION OPERATIONS

Definition: *Actions taken to affect adversary information and information systems while defending one's own information and information systems.*

Comment: Information Operations has been established in DoD policy as the overarching term to replace the former umbrella term Information Warfare. Consequently, a number of sources dealing broadly with the subject, but entitled Information Warfare, are cited in this subject area. Information Warfare is, however, a bibliographic subject area under which sources deal (consistent with DoD

terminology and concepts) with application of IO in specific real world crisis situations, e.g., Bosnia.

Bibliography Listing

Information Operations
Department of Defense Directive S-3600.1
December 9, 1996
This directive is the principal statement of Information Operations and Information Warfare policy, definition, and responsibilities within the Department of Defense. It establishes Information Operations as the overarching concept involving actions taken to affect adversary information and information systems while defending one's own information and information system. Information Warfare is established to be IO fenced in situation (*crisis* or *conflict*) and focus (*objectives over a specific adversary* or *adversaries*).

Joint Vision 2010
Chairman of the Joint Chiefs of Staff
1996
Joint Vision 2010 presents the conceptional template for how America's Armed Forces will channel the vitality and innovation of the American people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. It addresses the expected continuities and changes in the strategic environment including technology trends and their implications for the Armed Forces. The vision of future warfighting embodies the improved intelligence and command and control available in the information age and goes on to develop four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics. It cites an array of dynamic changes in the future environment and notes that our responses to dynamic changes concerning potential adversaries, technological advances and their implications, and the emerging importance of information superiority will dramatically affect how well the Armed Forces can perform their duties in 2010. The imperative of information superiority is defined as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information Warfare: A Strategy for Peace...The Decisive Edge in War
Joint Chiefs of Staff
Information booklet aimed at giving an overall idea behind the concept and implementation of Information Warfare, both defensive and offensive. Distributed by the Joint Chiefs of Staff, it focuses on the DoD perspective. The full-color, diagram-rich layout of the booklet makes it particularly helpful to those who are more visually oriented.

Joint Information Warfare Policy (U)
Chairman of the Joint Chiefs of Staff Instruction
CJCSI 3210.01, SECRET
2 January 1996
Provides joint policy and guidance for information warfare for application to the Joint Staff, Services, combatant commands, defense agencies, and joint and combined activities. Provides guidance concerning related capabilities, intelligence support, technology, training and education, joint operations plans, and legal issues.

Joint Doctrine for Information Operations
Joint Publications 3-13
Joint Chiefs of Staff
In preparation
This publication is to provide the U.S. military with overarching guidance for handling information operations. It is to be authoritative in that it is to be followed throughout military forces except when the warfighting commander decides that circumstances demand otherwise.

Joint Publication 3-13.1
Joint Chiefs of Staff
February 7, 1996
Information Warfare capitalizes on the growing sophistication, connectivity, and reliance on information technology and supports the national military strategy during both offensive and defensive situations. Command and control warfare is a warfighting application of IW in military operations and employs various techniques and technologies to attack or protect command and control. This publication does the following: provides an introduction to the fundamentals of IW; explains the elements of C2W; discusses intelligence support to C2W; covers joint C2W organization; covers command and control planning; describes C2W training and exercises; and explains C2W in multinational operations.

Joint Doctrine for Command and Control Warfare (C2W)
Memorandum of Policy No. 30 (MOP 30)
Command and Control Warfare
Chairman of the Joint Chiefs of Staff
Issued July 17, 1990, 1st Revision March 8, 1993
Superseded substantively by CJCSI 3210.01, Joint Information Warfare Policy 2 January 1996, Joint Pub 3-13, Joint Doctrine for Information Operations, in preparation; and Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare, 7 February 1996.
Current statement of joint policy concerning C2W. The provisions of this MOP apply to the Joint Staff, Services, unified and specified commands, defense agencies, and joint combined activities. The objective of these policies is to maximize U.S. and allied military effectiveness by integrating C2W into military strategy, plans, operations,

exercise, training, communications architectures, computer processing, systems development, and professional education. The key to successful C2W, according to MOP 30, is its integration throughout the planning, execution, and termination phases of all operations.

Information Operations Field Manual, FM 100-6
Headquarters, Department of the Army
August 1996
(from the preface) "This manual addresses the operational context of information operations (IO), relevant terminology, and the environment of information operations. It supports battle command and provides guidelines for commanders that conduct IO to support all phases of the force-projection operating environment, including planning and executing early entry and force-projection operations in joint and multinational settings."

Cornerstones of Information Warfare
Department of the Air Force
Document giving background information about information warfare and how it relates to Air Force military functions specifically. Distinguishes between direct and indirect information warfare as well as describes the components of IW: psychological operations, electronic warfare, military deception, physical destruction, and security measures. Applications to the Air Force include C2W and overall IO. This paper serves as the general Air Force background on information warfare.

OPNAVINST 3430.25, Information Warfare and Command and Control Warfare
Department of the Navy

OPNAVINST 3430.26, Implementing Instruction for Information Warfare
Department of the Navy

Marine Corps Order 3430.5A, Policy for Command and Control Warfare
Headquarters, Marine Corps

Electronic Warfare (EW) and Command, Control and Communications Countermeasures (C3CM)
Department of Defense Directive 3222.4
July 31, 1992
This directive updates the administration of and organizational responsibilities for EW and C3CM in the Department of Defense. This directive applies to the Office of the Secretary of Defense (OSD), military departments, Chairman of the Joint Chiefs of Staff and the Joint Staff, unified and specified commands, and the defense agencies.

Information Warfare: An Overview
W.J. Barlow, IDA Paper P-3030
Institute for Defense Analyses (IDA)
1801 N. Beauregard St.
Alexandria, Virginia 22311-1772
April 1995
Identifies and examines the concepts and relevant activities associated with DoD's recent initiatives on information warfare. Its purpose is to "provide a foundation and useful starting point from which IDA may subsequently assist the DoD in addressing issues of Information Warfare requirements, strategy, acquisition, and implementation." Points of interest include: contemporary views on IW, an approach for IW planning, and the elements of C2W and how C2W can be used as a military strategy.

Status of Command, Control and Communications Countermeasures (C3CM) Implementation within the Department of Defense (U)
IDA Report R-312, SECRET
Institute for Defense analyses
1801 N. Beauregard Street
Alexandria, Virginia 22311-1772
March 1988
Documents the progress made to implement the C3CM policy directed by DoD Directive 4600.4 and Joint Chiefs of Staff Memorandum of Policy Number 185. The study reviews the actions and responsibilities assigned by those documents and summarizes work completed by OSD, the JCS, Services, unified commands, and defense agencies to implement C3CM. The report includes a synopsis of Defense Science Board and DoD Working Group on C3CM recommendations that led to the C3CM policy. C3CM was the title given to the initial U.S. concept for the integrated use of operations security, military deception, jamming, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary C3 capabilities and to protect friendly C3 against such action.

Jane's Special Report: U.S. Information Warfare
Dr. George Stein, with contributions from Col. Richard Szafranski, USAF (Ret.)

This report provides one of the best comprehensive introductions to IW available. Stein includes a history of the information age, a conceptual overview of IW, organizational concepts (including an assessment of Joint Vision 2010 and a comparison of IW to air and space power), resistance to IW, suggestions and initiatives on the road to a national IW strategy, and information models for the 21st century. The concept of information superiority is explored, as are topics such as ethics of IW and military resistance to IW. An extensive bibliography is cited, including a special section for Government publications and laws. An acronym list and a glossary are also provided.

Waging the Infowar
Jane's International Defense Review Extra
J.R. Wilson
April 1997
Information Warfare is reviewed from many angles, with reference to the different service perspectives, national policy, civil sector, and international politics. Both components of IW-O (offense) and IW-D (defense) are addressed. Examples of implementation of these concepts are given, including actions taken both in the Persian Gulf and in the China-Taiwan response of early 1996. A brief review of the Defense Science Board Task Force's report on "Information Warfare - Defense" is given, highlighting the numerous areas from which an information attack could come. The question of and possible answers to who should be responsible for defense are raised (but, of course, not resolved), and reference is made to the ultimate goal of "information supremacy" as described by the Joint Chiefs of Staff's *Joint Vision 2010.* Information warfare—both offensive and defensive—is, according to this review, "not merely a wartime activity or battlefield element but is, like its sub-element espionage, an ongoing effort in times of peace as well as war.... All of this raises new questions of international and domestic law, privacy, constitutional rights, treaties, and, of course, politics."

Information Warfare Series
SIGNAL
A compendium of articles from the May, June, and July 1996 issues of *SIGNAL*
The series can be ordered by visiting the site: http://www.us.net/signal/Infowar/infowar.html
The series serves as an overview of current issues involved in the study and development of information warfare capabilities by addressing areas in theory, technology, national policy, defense policy, and implementation.

Business and Government issues are addressed, topics include:
Issues of privacy and security, National Information Infrastructure, transfer of defensive information warfare technology to industry.

Some *military strategy* is explained:
Force XXI, The Enterprise Vision, and Command and Control Protect.

Coverage in the articles *also includes*:
Land Information Warfare activity, Air Force Information Warfare Center, Fleet Information Warfare Center, Computer Emergency Response Team, Defense Information Systems Agency, National Imagery and Mapping Agency, escrowed encryption standard, multilevel information systems security initiative (MISSI), and Fortezza encryption card.

Characteristics of Information Warfare, Information Warfare Panel 1
Fred Giessler, Ph.D., Thomas P. Rona, George F. Kraus, Jr., Lt. Col. Mike Brown
February 8, 1995
Notes from all of the speakers at an IW panel discussion. The specific topics include Characteristics of IW, Characteristics of IW by AFCEA, Information War: Russian

Views, and Concepts for the Future. This packet is arranged in slide format and explanations and discussions are not included.

B. DEFENSIVE INFORMATION OPERATIONS

Definition: *A process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counterdeception, counterpsychological operations, counterintelligence, electronic protect, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information on information systems for their own purposes.*

Comment: Also see listing in Section C, Information Assurance, and D, Infrastructure Protection, which are significant aspects of Defensive Information Operations treated separately because of their particular focus and the differing approach thereto within the U.S. Government.

Bibliography Listing

Defensive Information Operations Implementation
Chairman of the Joint Chiefs of Staff
CJCSI 6510.01B, 22 August 1997
Provides implementing guidance and supplemental joint policy for defensive information operations. The defensive IO process is described, and related policy, joint responsibilities, and procedures are established. An exhaustive list of applicable references and a glossary of relevant terms are included.

Information Architecture for the Battlefield
Report of the Defense Science Board Summer Study Task Force
Office of the Under Secretary of Defense for Acquisition and Technology
Washington DC 20301-3140
October 1994
This overview describes what global security and information warfare are and suggests areas in which attention must be focused so as to provide the maximum security and mobility for U.S. forces in the face of information attack or war. Suggestions include net assessment, investing in defense, red teaming, and commercial directives.

Information Warfare Threats to Automated Information Systems Threat Environment Description
Thomas J. Steinbrunner
National Air Intelligence Center, Wright-Patterson AFB, OH
April 1997
Presents the wartime threat environment that could confront U.S. automated data processing (ADP) assets. It addresses the wartime threat environment and contains threat information relevant to cyber attacks on a global basis.

C. INFORMATION ASSURANCE

Definition: *Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA.*

Comment: Information assurance is a significant aspect of defensive IO. It is treated here as a separate subject area because it is of major interest to Congress and within DoD, and it is frequently addressed as a separate subject area.

Bibliography Listing

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks
United States General Accounting Office, Accounting and Information Management Division
Report to Congressional Requesters
May 1996
Official report of the U.S. GAO to Congress about the extent to which Defense computer systems are being attacked, the actual and potential damage to the DoD information and systems, and the challenges Defense is facing in securing sensitive information. Defense Information Systems Agency (DISA) data implies that Defense may have experienced as many as 250,000 attacks last year and that attacks are successful 65 percent of the time. These numbers were generated based on DISA's Vulnerability Analysis and Assessment Program in which DISA personnel attempt to penetrate computer systems at various military service and Defense agency sites via the Internet. Real attacks are thought to occur in a variety of ways. The GAO states that "at a minimum these attacks are a multimillion dollar nuisance to Defense, and at worst, they are a serious threat to national security." Currently, Defense is attempting to react to successful attacks as it learns of them but has no uniform policy for assessing risks, protecting its systems, responding to incidents, or assessing damages. Chapter 4 of the report contains recommendations to the Secretary of Defense for ensuring that sufficient priority, resources, and top-management

attention are committed to establishing a more effective information systems security program—one that includes (1) improving security policies and procedures, (2) increasing user awareness and accountability, (3) setting minimum standards for ensuring that system and network security personnel have sufficient time and training to properly do their jobs, (4) implementing more proactive technical protection and monitoring systems, and (5) evaluating Defense's incident response capability. It also includes a recommendation to the Secretary for assigning clear responsibility and accountability throughout DoD for the successful implementation of the security program.

Information Assurance Task Force Interim Status Report
OSD lead: Mr. Roger Callahan, OASD(C3I); Joint Staff lead: Lt. Col. Bob Gorrie, J-6
January 27, 1997
(See the following entry for the final report on March 28, 1997.)
Slide-style presentation of research and recommendations about various DoD agencies that are or will be in control of information systems in the United States, especially those important to national security. Includes a segment on threat assessment, which examines levels of threat from incompetent blunders to major strategic disruptions of the United States on a timeline of today, by 2005, and beyond. Lists Defense Science Board (DSB) objectives and suggestions for immediate action.

Improving Information Assurance: A General Assessment and Comprehensive Approach to an Integrated IA Program for the Department of Defense
Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD C3I)
6000 Defense
Pentagon, Room 3E243
Washington, DC 20301-6000
Prepared by: R. Schaeffer, Jr., Chairman of the Information Assurance Task Force
(301)688-0840
March 28, 1997
(from the Executive Summary) "This report provides a general assessment of the Department's current IA posture and a comprehensive approach to achieving an integrated IA Program. The general assessment, while pointing to significant deficiencies within the Department's IA posture, acknowledges the benefit of ongoing IA initiatives among the Defense Components and stresses that the Department must maintain and build upon this momentum. Seven program components are identified as the key areas in which action must be taken. These seven programs are readiness assessment, human resources development, operational policy and doctrine, security management and operational monitoring, architectural standards and system transformation, acquisition support and product development, and research and technology. The Task Force suggests that investing in these program components will collectively enhance the IA capability for mission readiness."

DoD Directive 8000.1, Defense Information Management Program
Office of the Secretary of Defense
October 27, 1992
Director, DISA will "in consultation with the Directors of the DIA and NSA, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of defense information, commensurate with its intended use."

Planning Considerations for Defensive Information Warfare—Information Assurance
Task Order 90-SAIC-019
December 15, 1993
Critical review of the Defense Information Infrastructure (DII) and the need to create and maintain information assurance policies for security reasons. Suggestions for course of action include the development of information assurance doctrine, strategy, tactics, techniques, and procedures as well as information assurance standards, technologies, tools, and guidelines. The review also addresses issues of cost effectiveness and reasons for the need to implement information assurance as DII is being created.

Risk-Free Access into the Global Information Infrastructure Via Anonymous Re-Mailers
by Paul S. Strassmann, U.S. Military Academy, West Point, and Senior Advisor, SAIC and William Marlow, Senior Vice President, SAIC
"Symposium on the Global Information Infrastructure: Information, Policy & International Infrastructure Cambridge," MA, January 28–30, 1996
Available online at: http://www.strassmann.com/pubs/anon-remail.html
Precise description of anonymous re-mailers, which are of vital interest to anyone involved in security of the Global Information Infrastructure. An anonymous re-mailer is a program that runs on a computer somewhere on the Internet and allows anyone to post messages to newsgroups or individuals while remaining anonymous. The identity of the sender is hidden from the recipient and remains practically untraceable. This method of communication is a favorite for engaging services of cybercriminals and for authorizing payment for their acts through a third party. This detailed report is written for the purpose of making policymakers aware of the wealth of, as well as the dangers of, the use of anonymous remailers.

Spectre Press
"The World's Most Dangerous Catalog"
available online at: http://www.spectre-press.com/
This catalog is one of a number of resources designed to provide instruction in fields that could be dangerous to national security. As described in the introduction to the homepage, this catalog "specialize[s] in the fields of Electronic Warfare, Hacking, Nuclear and Conventional Weaponry, Phreaking, Energy, Spy Weaponry, Virii, Banking, and Personal Defense." The distributors who maintain the homepage and the products

caution that, "You may find some of our products controversial or upsetting, others you may find necessary to possess. Spectre Press believes that distribution of this information is in the vital interest of the people. Although illegal methods may be thoroughly described in precise detail, no illegal method is suggested or implied. All products are for educational use only!"

National Security Directive 42
July 5, 1990
NSD 42 addresses U.S. Government capabilities for securing national security systems against technical exploitation and implementing countermeasures. The Secretary of Defense is executive agent and the Director of NSA is designated as the National Manager and charged with examining national security systems and evaluating their vulnerability. Defines telecommunications, information systems, and national security systems. Reestablishes the National Security Telecommunications and Information Systems Security Committee (NSTISSC). NSTISSC is tasked to develop policies, procedures, guidelines, instructions, standards, objectives, and priorities and systems security guidance; to approve the release of cryptographic material to foreign governments with CIA concurrence; to establish a national system for promulgating operating policies, instructions directives, guidance, etc.; and to interact with the National Communications Systems' Committee of Principals established by Executive Order 12472. NSA provides a supporting secretariat.

D. INFRASTRUCTURE PROTECTION

Definition: *Set forth by Executive Order 13010 and the President's Commission on Critical Infrastructure Protection (PCCIP) as: The National Infrastructure is the framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a flow of goods and information services essential to the defense and economic security of the United States. "Critical infrastructures" are deemed to be so vital that the incapacity or destruction of key components would have a debilitating regional or national impact. They include:*

- *Electronic power systems*
- *Gas and oil*
- *Telecommunications*
- *Banking and finance*
- *Transportation*
- *Water supply systems*
- *Continuity of Government services*
- *Emergency services (medical, police, fire, rescue)*

Comment: Infrastructure Protection is a significant aspect of Defensive Information Operations at the national level. It deals with the protection of the information and information systems essential to

the functioning of a variety of infrastructures critical to the national security and economic interests of the United States. Such infrastructures include transportation, power generation and distribution, and national information.

Bibliography Listing

Report of the Defense Science Board Task Force on Information Warfare - Defense (IW-D)
Defense Science Board
Office of the Under Secretary of Defense for Acquisition and Technology
Washington, DC 20301-3140
November 1996
available online at: http://jya.com/iwdmain.htm
The Defense Science Board Task Force on Information Warfare (Defense) was established at the direction of the Under Secretary of Defense for Acquisition and Technology. The Task Force was directed to focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare-defensive (IW-D) capability in several areas, including deterrence. Specifically, the Task Force was asked to identify the information users of national interest who can be attacked through the shared elements of the National Information Infrastructure (NII); determine the scope of national information interests to be defended by IW-D and deterrence capabilities; characterize the procedures, processes, and mechanisms required to defend against various classes of threats to the NII and the information users of national interests; identify the indications and warning, tactical warning, and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize attacks on the NII; identify the reasonable roles of Government and the private sector, alone and in concert, in creating, managing, and operating a national IW-D capability; and provide specific guidelines for implementing the Task Force's recommendations. Key issues addressed include the necessity to be able to perform critical functions even in the presence of IW attacks; a minimal essential infrastructure capabilit,y which would support these functions; point and layered defenses rather than area defenses; a defense system which is able to function in the presence of failed components, systems, and networks, and a separate infrastructure control unit that is not dependent on normal operation of the infrastructure. In addition, the Task Force states that the infrastructure must be capable of being repaired. Thirteen key recommendations are made, including increasing awareness of IW-D, assessing vulnerabilities and readiness of current security measures and providing the resources needed for a project of this magnitude to continue efficiently and effectively. The Task Force states that the basic functions of monitoring, detection, damage control, and restoration must be possible at the lowest possible level to serve the above purposes.

Defensive Information Warfare Study ISAT-95
Defense Advanced Research Projects Agency (DARPA)
This study addresses potential technology paths for mitigating the situation created by national dependence on civil information systems by improving the inherent robustness of such systems. This approach is particularly important since information-related vulnerability is not limited to directed attacks, but extends to situations in which large-scale failures of non-malicious origin may occur as a result of simple technological failures. The study was performed by three case study teams and a robust enterprise engineering team. The case studies focused on (1) electrical power, telecommunications, and financial services, (2) the understanding of information system dependencies and vulnerabilities, and (3) identifying common research drivers. The case study teams were, in essence, to survey the information system dependencies and vulnerabilities of these representative civil enterprises to attempt to distill common research issues. The engineering team undertook to evolve toward an engineering discipline for a large-scale, distributed, information-dependent system, to consider both near and longer term priorities, and to identify essential research gaps.

Interagency Terrorism Response Awareness Program (I-TRAP) VI Reference Manual
Prepared for the Assistant Secretary of Defense (Special Operations and Low-Intensity Conflict)
Department of Defense, Pentagon, Washington DC 20301
Prepared by Kapos Associates Inc., Arlington, VA
January 27, 1997
This reference manual was compiled for the use of participants in I-TRAP VI and is organized in four major sections: The Physical and Informational Infrastructures; Understanding the Threat and Associated Vulnerabilities of the Information Infrastructure; Organizations and Response Capabilities; and Authorities. This report provides an excellent overview of current issues in question in the field of information assurance as it pertains to national policy. The idea of "critical information infrastructures" is addressed, with reference to Executive Order 13010, July 1996.

Electric Power Information Assurance Risk Assessment
Information Assurance Task Force
National Security Telecommunications Advisory Committee
March 1997
This is a risk assessment conducted by the Information Assurance Task Force (IATF) of the National Security Telecommunications Advisory Committee (NSTAC). It includes interviews and discussions with a wide range of representatives from the electric power industry. It is an excellent compilation of threat, vulnerability, and potential responses for this subject area. The report closes with a number of recommendations for the President, the electric power industry, and NSTAC.

CONOPS - Department of Defense Computer Crime Unit Concept of Operations
Special Agent Jim Christy
Department of Defense Representative
DOJ's Infrastructure Protection Task Force
FBI HQ, Washington DC
January 14, 1997
Proposal to create a DoD Computer Crime Unit (CCU) to serve as a centralized network that oversees all organizations involved in the areas of computer crime and computer intrusion investigations. The proposal provides an estimate of manpower required to support DoD CCU mission areas of policy, training, computer forensics, computer intrusion investigations, and specialized legal expertise. Funding considerations, functional areas, and phasing of manpower are addressed.

The Nuclear Black Market
Global Organized Crime Project
Center for Strategic and International Studies (CSIS) Task Force Report
1800 K Street, N.W., Washington, DC 20006

Overview of this report and helpful links available at:
http://www.csis.org/html/pubsecur.html#nukeblack
An element of information assurance is knowledge of resource availability and the ability to deter theft of materials dangerous to the safety and security of U.S. forces or citizens. The Global Organized Crime Project was created by the Center for Strategic and International Studies (CSIS) to assess security in various areas, one of which is the Nuclear Black Market. The purpose of the Nuclear Black Market Task Force was to first assess the threat, then the safeguards and security at the source, and finally look at the areas that come into play when prevention fails: detection, interdiction, and neutralization. This type of study provides an excellent parallel of the practical application to both the defense and commercial sectors in the area of infrastructure protection.

Awareness of National Security Issues and Response (ANSIR) Home Page
Found online at: http://www.fbi.gov/ansir/ansir.htm
The FBI program ANSIR disseminates information concerning national security matters. Eight "key issue threats," which are under the jurisdiction of the FBI to respond to and investigate, are detailed: terrorism, espionage, proliferation, economic espionage, targeting the National Information Infrastructure, targeting the U.S. Government, perception management, and foreign intelligence activities. Each threat is characterized and described for the purpose of delineating the FBI's jurisdiction in these matters.

E. INFORMATION SYSTEM

Definition: *Defined by DoD Directive S-3600.1, 1 December 1996 as "The entire infrasturcture, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."*

Comment: This category is intended to provide a sharper understanding of what constitutes the defended set of resources. The Directive tasks all DoD components to "work toward a multilayered information systems defense that incorporates protection, detection, reaction, and reconstitution." It also notes that DoD information systems critical to the transmission and use of minimum essential information for command and control of forces shall be designed, employed, and exercised in a manner that minimizes or prevents exploitation, degradation, or denial of service.

Bibliography Listing

C4I for the Warrior
Global Command and Control System: From Concept to Reality
J-6 Joint Staff, Pentagon
June 1994
Handbook and information guide, which explains the concepts of the GCCS. The GCCS is evolving to be the joint C4 system of C4 systems, interoperable through common paths and common switches. This system of systems is part of the puzzle that must be assembled to give the joint forces commander a true picture of the battle space in real time. "The brochure focuses on the GCCS, the support it was receiving in 1994, and the progress being made in transforming the C4I for the Warrior vision into reality for today's and future warriors." (from the preface)

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)
Chapter 27 of Annual Report to the President and Congress from Secretary of Defense
March 1996
This chapter deals with the development of a C4ISR architecture and the necessary elements for this project. The report includes information about command and control (C2), the Defense Information Infrastructure (DII), information systems security, and intelligence/counterintelligence, among other things. C4ISR-related defense agencies are listed and described, including CIA, DIA, DIS, DISA, DMA, NRO, and NSA.

Joint Precision Interdiction
Report of the Defense Science Board
for the Office of the Undersecretary of Defense for Acquisition and Technology
June 1994
This report appraises the status of technologies and supporting programs to carry out the JPI mission. There are (or have been) many very successful developments that provide implementations of the battlefield intelligence, target acquisition, weapons delivery systems, munitions and battle damage assessment functions required for JPI. The information systems and interoperable communications needed to tie the system elements together in the joint operational environment are lacking, and obtaining such capabilities has been a persistent problem. The recommended option is for OSD to continue to place its emphasis on the compatible information systems aspects of developing Joint Precision Interdiction (and/or Strike) capabilities. Another recommendation is that the OSD provide focused leadership to keep in place all elements of this complex of development and acquisition activities.

Tactical Air Warfare
Report of the Defense Science Board
Office of the Under Secretary of Defense for Acquisition and Technology
Washington, DC 20301-3140
November 1993
Recommendations that DoD implement an information infrastructure (DoDII) to assist Tactical Air Warfare. Includes suggested hierarchy of the DoDII distribution system, which would eliminate redundant information gathering by the three Services. Also highlights the vulnerability of commercially built and/or owned communications tools such as satellites and computer systems, networks, and software.

F. INFORMATION WARFARE

Definition: *Information Warfare was redefined by DoD Directive S-3600.1 on 9 December 1996 to read that IW is "Information Operations (IO) conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." IO is defined to be "actions taken to affect adversary information and information systems while defending one's own information and information systems."*

Comment: The foregoing Directive greatly narrows the scope and content of the previous definition of Information Warfare and substitutes "Information Operations" as the new umbrella term that encompasses most of the concepts and activities formerly assigned to "Information Warfare."

Bibliography Listing

Implementation of a C3 Countermeasures (C3CM) Strategy in Korea (U)
IDA Report R-363, SECRET
Institute for Defense Analyses
1801 N. Beauregard Street
Alexandria, Virginia 22311-1772
June 1990
Outlines the functions, processes, and responsibilities for activities in Korea related to C3CM planning and implementation. Emphasis is on C3CM concept of operations; target nominations, analyses, and selection; integration of C3CM elements; information sources and flows; options/payoff analysis; and feed back mechanisms. A baseline description of the C3CM functional process in Korea is established to include the use and potential use of automated aids to assist the C3CM mission. Features of the C3CM process in use in Korea were identified which could serve as a useful model for incorporation by other Joint and Combined Commands.

Command, Control, and Communication Countermeasures (C3CM) During DESERT SHIELD/DESERT STORM (U)
IDA Paper P-2678, SECRET
Institute for Defense Analyses
1801 N. Beauregard Street
Alexandria, Virginia 22311-1772
June 1992
U.S. and Coalition operations during Desert Storm involved the first significant use of a C3CM strategy and associated principles since implementation of the DoD directive and policy promulgated in 1979. The study researched and presented the details of five selected case studies that illustrated the full range of Counter-C3 and C3-Protect activities. Coupled with analyses of national and theater level C3CM organization and processes, the who, how, and what of the major C3CM events of the Gulf War are provided. Based on the analyses conducted, the paper concludes that C3CM was indeed an unprecedented success, but indicated a number of actions that would improve the conduct of C3CM in future conflicts.

The First Information War
Contributing Editor, Alan D. Campen
Published by AFCEA International Press (AIP)
October 1992
Compilation of articles, mostly from *SIGNAL* magazine, detailing the role of information and knowledge during the Persian Gulf War. Campen provides a useful summary of each essay in the preface, pages vii to xxi. These summaries allow the reader to choose topics that may be the most useful in his/her search; topics range from Information Systems and Air Warfare to Extending Real-Time Intelligence to Theater Level.

Information Operations in Bosnia : A Preliminary Assessment
Strategic Forum 91, National Defense University's Institute for National Strategic Studies
Kenneth Allard
November 1996
Allard addresses a variety of topics, and presents a summary of his remarks at the beginning of his paper. In his opinion, coordination in Bosnia has been handicapped because the Dayton Accords did not designate a single authority to synchronize the military, political, and humanitarian aspects of the mission. Because the Information Revolution largely stops at division level, high technology systems support the headquarters far more effectively than the soldier on the ground. The Bosnian experience underlines the need to substitute commercial telecommunications, automation and services for outmoded military equipment and support structures. And finally, much of the success of the Bosnian operation can be traced to the quality of the American soldier, especially in his innovative use of both commercial and military technology. Allard cautions that "the Bosnian experience should remind us that our worship of technology in warfare must be tempered by a stronger sense of the human factor."

Bosnia's Information River Slows, Trickles to Soldiers
SIGNAL
Clarence A. Robinson, Jr.
June 1997
Discusses the question of where IW has actually begun to be used and suggests that this shift toward better access to information and more strategy than physical conflict in wartime is only apparent at the "top" of the proverbial totem pole. It is suggested in quotations by Kenneth Allard that the information revolution has had little effect on the way operations are handled in the field. Much of the focus of this problem, it is suggested, is the military hierarchical mentality. The technology exists for people at many levels to access information, but this technology is not being adequately applied. So as to preserve the chain of command, efforts are not being made to allow universal access to information. Allard maintains that the organizational implications of modern warfare must be addressed; synchronizing the political and military sides of a peace-keeping operation, reducing top-heavy headquarters and substituting commercial products for outmoded military equipment and redundant support structure.

The Information Warfare Campaign Builder & Analysis Tool (IW CBAT) Version 2.0
Reference Guide
March 1997
ANSER, Arlington, VA
In wide use by the Joint Staff, this software gives its users the ability to construct and analyze an Information Warfare campaign from a personal computer. Options included in this program include recording assessments of importance of various goals, objectives, strategies, and tasks with respect to specific IW campaigns (importance assessments);

recording assessments of level of confidence in accomplishing the IW tasks (capabilities assessments); viewing the entire campaign as it is being constructed; adding or deleting goals, objectives, strategies, and tasks; and printing reports of assessments for instructional purposes. According to the Reference Guide, the IW CBAT is based on a comprehensive hierarchy of information warfare goals, strategies, objectives, and tasks, which are explained in a document accompanying the software. The software is generic in nature so as to be useful in both Red and Blue team planning exercises, and is diverse enough to allow a large range of different scenarios; it can be focused on a specific phase in a crisis or conflict or can be used as an integrated effort over the entire conflict spectrum.

G. NATIONAL POLICY

Bibliography Listing

A National Security Strategy of Engagement and Enlargement
Prepared by the President
The White House
February 1996
Presents the U.S. national security strategy. Recognizes that the threat of intrusions to our military and commercial information systems poses a significant risk to national security and notes that this matter is being addressed.

Executive Order 12333, United States Intelligence Activities
The White House
December 4, 1981
Intelligence effort to provide necessary information on which to base decisions to the President and to protect national interests from foreign security threats. Special emphasis to countering espionage directed against U.S. Government, corporations, establishments, or persons. Secretary of Defense was named executive agent for signals intelligence and communication security activities. NSA is to execute the responsibilities of the SecDef as executive agent for communications security and to conduct research and development as necessary for signals intelligence and communications security. The Department of Energy will support NSA as requested. Restricts collection techniques to procedures established by the agency head and approved by the Attorney General.

Executive Order 12382, President's National Security Telecommunications Advisory Committee
The White House
September 13, 1982
Establishes the National Security Telecommunications Advisory Committee to provide the President with advice and information from the perspective of industry with respect to national security telecommunications.

Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunication Functions
The White House
April 3, 1984
Establishes the National Communications System (NCS), an interagency group made up of 23 Federal departments and agencies. The NCS is responsible for ensuring that NS/EP telecommunications are available across a spectrum of national emergencies. NCS is to serve as a forum for Government agencies and private sector. To facilitate this process, EO 12472 establishes the Committee of Principals for the Federal Government to coordinate with the National Security Telecommunications Advisory Committee consisting of industry representatives.

Executive Order 12658
Assignment of Emergency Preparedness Responsibilities
November 18, 1988
Policy delineating the necessity of and responses to a "national security emergency," which includes natural disaster, military attack, technological emergency, or other emergency that seriously degrades or seriously threatens the national security of the United States. As used in this Order, preparedness functions and activities include, as appropriate, policies, plans, procedures, and readiness measures that enhance the ability of the U.S. Government to mobilize for, respond to, and recover from a national security emergency. Also see Executive Order 12472.

Executive Order 12958, Classified National Security Information
The White House
April 17, 1995
This EO revoked EO 12356. It has two major purposes: (1) to prevent unauthorized disclosure of information and (2) to prevent over-classification of information. It prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The EO provides 5 years for the Services and others in DoD to review all documents more than 25 years old and to request waivers, on a document by document basis, if the documents are not to be declassified automatically in 2001. The Office of Management and Budget (OMB) is tasked with issuing implementing directives in coordination with the Security Policy Board and the Assistant to the President for National Security Affairs. It establishes within the OMB the Information Security Oversight Office (previously an office in GSA) to implement and monitor the program on behalf of the Director, OMB. It also establishes the Information Security Policy Advisory Council. As a Federal Advisory Committee, the Council is to advise the President and other members of the Executive Branch on security policies and to provide recommendations to agency heads for specific subject areas for declassification review.

Executive Order 13010
President's Commission on Critical Infrastructure Protection
July 15, 1996
(from the introduction) "Certain national infrastructures are so vital that their incapacity or destruction would have debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue) and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications component that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation." This Order created the President's Commission on Critical Infrastructure Protection to address these issues at the national level, as well as an interim acting body called the Infrastructure Protection Task Force (IPTF), chaired by the FBI. The IPTF is to increase coordination of existing infrastructure protection efforts in order to better address and prevent crises that would have a debilitating regional or national impact.

Federal Response Plan
Public Law 93-288
April 1992, Revised 1996
available online at: http://www.fema.gov/library (from this page the document can be found in the index)
This plan, created in concert with the Federal Emergency Management Agency (FEMA), proposes to facilitate delivery of all types of Federal response assistance to States to help them deal with consequences of "significant disasters." The plan outlines planning assumptions, policies, concept of operations, organizational structures and specific assignments of responsibility to departments and agencies in providing Federal assistance to supplement State and local response efforts. The plan provides an excellent structural framework for both the description of and the means to deal with significant disasters, making it an ideal outline to use for creating policy about dealing with information infrastructure attacks or failures. The "information infrastructure" is not discussed per se because, at the time of its creation, the information infrastructure was less developed.

Presidential Decision Directive 29
The White House
1994
The directive states that a new security process is required and that the process should be based on sound threat analysis and risk management practices.

Presidential Decision Directive 39
The White House
1995
This directive calls for protection of certain critical infrastructures. Infrastructures such as those associated with transportation, power generation and distribution, and national information are considered critical because they support national and economic security interests of the United States.

H. PERSPECTIVES

Bibliography Listing

Joint Vision 2010
Chairman Joint Chiefs of Staff
1996
Joint Vision 2010 presents the conceptional template for how America's Armed Forces will channel the vitality and innovation of the American people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. It addresses the expected continuities and changes in the strategic environment including technology trends and their implications for the Armed Forces. The vision of future warfighting embodies the improved intelligence and command and control available in the information age and goes on to develop four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics. It cites an array of dynamic changes in the future environment and notes that our responses to dynamic changes concerning potential adversaries, technological advances and their implications, and the emerging importance of information superiority will dramatically affect how well the Armed Forces can perform their duties in 2010. The imperative of information superiority is defined as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

A Theory of Information Warfare: Preparing for 2020
Colonel Richard Szafranski, USAF
This article can be found online at: http://www.cdsar.af.mil/apj/szfran.html
This article is also included in *Cyberwar: Security, Strategy and Conflict in the Information Age*, a compilation of articles from *SIGNAL* magazine (see below).
(review by the Airpower Journal) "How should we wage information warfare at the strategic and operational levels? What moral and ethical considerations are there? Information technology may now have evolved where "control" can be imposed with little physical violence or bloodshed. On the surface this may appear to be a good thing. At its core this may be a dangerous thing. Closer scrutiny should reveal which of these is the case."

Battlefield of the Future: 21st Century Warfare Issues
http://www.cdsar.af.mil/battle/bftoc.html
This webpage provides a table of contents linking the reader to numerous selected chapters of books on current warfare issues including what the battlefield of the future looks like, airpower issues, and both information and biological warfare. The Table of Contents is organized by subject heading, and the Information Warfare Overview can be found at: http://www.cdsar.af.mil/battle/ov-6.html
Two chapters are listed to describe this field. George J. Stein's Chapter 6, "Cyberwar—Netwar," of *Information War* is cited at: http://www.cdsar.af.mil/battle/chp6.html
The second chapter found under this heading is "Information Warfare: Impacts and Concerns," written by Col. James W. McLendon, USAF, and found at: http://www.cdsar.af.mil/battle/chp7.html

Command, Control, and the Common Defense
Kenneth Allard
National Defense University, Institute for National Strategic Studies
Revised Edition published in 1996
Allard's book provides a look at command and control communications in the post-Desert Storm Armed Forces. He proposes to answer the question: How do the pluralistic traditions of service autonomy, which are a major part of the American military experience, affect the way in which command is exercised over our combatant forces, now and in the future? Of interest to those involved in information warfare research is the Epilogue, Desert Storm and Information Age Warfare (Chapter 9). This chapter looks at information warfare in the context of what is considered "the first information war." A concise description is given of what the United States did during Desert Storm that created the level of information dominance attained during the conflict. This description is followed by a broader look at "the revolution in military affairs," in areas like interoperability, communications infrastructure, intelligence, institutional responses, operational factors, cultural and generational factors, and commercial and industrial factors. Allard cites two areas of consensus, (1) information systems are useful only to the extent that they reduce the fog of war and (2) the command structure must be capable of winning even after the computer dies.

Cyberwar: Security, Strategy and Conflict in the Information Age
Contributing Editors: Alan D. Campen, Douglas H. Dearth, R. Thomas Goodden
© May 1996 AFCEA
Compilation of articles, mostly from *SIGNAL* magazine, which examine the realm of cyberspace and the role of the information warrior. The articles are grouped into four parts, each of which examines a different level of IW. *The Information Age in Historical Perspective* includes articles that summarize societal and military changes that have led to the creation of a sphere called IW. *Cyberwar and Civil Society* addresses elements of IW that pertain both to the larger society and the military, including the role of the United States in cyberspace, business strategies in the Information Age, and the role of the media. *Organizing for Cyberwar* is focused primarily on the role of the military and

different perspectives on how the military should ready itself for an information war. *Warfare in the Information Age* provides an overview of issues that confound studies in this area, including ethical issues and problems with the security of national policy. A short summary of each article is included in the introduction, and a suggested reading list is included at the end of the book.

Defending Cyberspace and Other Metaphors
Martin C. Libicki
National Defense University, Institute for National Strategic Studies
Center for Advanced Concepts, Technologies, and Information Strategies
February 1997
Libicki cautions his readers not to overreact to the threat of information attack, but to realize that information warfare is, in fact, a phenomenon that must be understood separately from warfare as a whole. He uses metaphors to clarify the concepts involved in information warfare but reminds his readers that "to use metaphor in place of analysis verges on intellectual abuse." Six essays are presented "in the continuing search for the meaning of information warfare." The main foci of his essays investigate (from the introduction): "(1) the risks to national security bred by dependence on infrastructure, which Libicki claims are easily overstated, (2) whether an explicit policy of retaliation is workable and thus easy to deter, (3) the gap between what information warfare can do and what it can appear to do and whether that gap can be exploited for psychological warfare, (4) the similarities between information warfare and Cold War mindsets, (5) parallels between information warfare and the human immune system, in which the immune system is revealed "as an information-warfare machine that uses a rich selection of redundancy, fail-safe devices, stimulants, and suppressers" to attack foreign antigens but not attack the human body, and (6) the change in warfare from "lines" (e.g., front line, line of defense) to "points, blots, and gated fences" (e.g., precision strikes, small-scale take-overs, and the containment of those take-overs). This last analogy is Libicki's search for a new metaphor for a new kind of warfare."

Defensive Information Warfare
David S. Alberts
National Defense University, Institute for National Strategic Studies
Center for Advanced Concepts, Technologies, and Information Strategies
August 1996
Alberts uses the term "information strategies" to refer to the recognition and utilization of information and information technologies as an instrument of national power that can be independent of, or complementary to, military presence and operations. Thus, Information Warfare – Defense (IW-D) might more aptly be named IWS-D. Alberts' overview of IW-D "does not attempt to deal with the problems of defending against all of the different kinds of information attacks, but rather focuses its attention on the subset of IW that involves attacks against our information infrastructure, including what has become known as 'hacker warfare' and in its more serious form, 'digital warfare.'" Two

main goals are highlighted: finding a way to protect ourselves against catastrophic events and building a firm foundation on which we can make steady progress by continually raising the cost of mounting an attack and mitigating the expected damage. Alberts outlines a framework for progress, which includes such vital components as awareness of the threat, cooperation, delegation of fixed responsibilities, and the implementation of "rules of the game." Other areas addressed include Alberts' suggested allocation of responsibilities and an organizational action plan.

The Information Revolution and National Security: Dimensions and Directions
Center for Strategic and International Studies (CSIS)
Ed: Stuart J.D. Schwartzstein
1996
Collection of articles relating to issues and implications of the information revolution on national security and to the topic of conflict in the information age. Of particular interest is a selected bibliography by C. Edward Pairtree covering the topics of: Implications of the Information Revolution, Information Security and Cybercrime, Information Revolution and the Military, and Law, Civil Society, and the National Interest: Conflict in the Computer Age. Some entries include an annotation for ease of reference, and electronic sources are cited as well.

Information Warfare Forum
Joint Chiefs of Staff, Arthur K. Cebrowski Vice Admiral, USN, Joint Staff/J6
January 1995
These briefing notes and figures provide a visual representation of the logic behind the use of Information Warfare as a defensive and offensive measure. A call to action is sounded in the areas of strategy, technology, fixing accessibility, and modeling.

Information Warfare is Rife with Promise, Peril
Col. Alan D. Campen, USAF (Ret.)
SIGNAL, November 1993
Campen's article cautions that "military leaders must understand which time-honored precepts of warfare are challenged by information-intensive combat. In addition, they also must decide if the military can ensure information dominance over the battlefield or if it should employ alternative force control methods. These leaders need to determine whether sophisticated electronic warfare tools can be effective against low-technology adversaries—fanatics or rogue nations that do not depend on free-flowing information." Campen raises numerous questions about the emerging role of technology as well as the repercussions this will have on traditional land warfare and engagement tactics. He does not propose to answer these questions, rather he sets the table for further debate and policy considerations to be made in this area.

Revolutionary Change in Warfare: A Review of Theories, Arguments and Policy Implications
Stephen D. Biddle, IDA Papaer P-3123
Institute for Defense Analysis (IDA), Strategy Forces and Research Division
1801 N. Beauregard St.
Alexandria, Virginia 22311-1772
September 1995
The paper provides a review of the literature on revolutionary change in warfare, a critique of that literature, and a series of recommendations for its further development. It argues that although an impressive consensus has developed that modern warfare is undergoing a revolutionary change, the analytical foundations for this thesis are significantly underdeveloped. Terminology is vague and ill-defined; imputed cause and effect relationships are mostly implicit and unexamined; supporting evidence is limited and often insufficient to sustain the conclusions reached. On the basis of the existing literature, it is impossible so far to establish whether the policy prescriptions it advances are sound. Plausible alternatives to the projections now dominate the debate and could imply a very different understanding of future warfare, with very different policy implications, yet these cannot be ruled out on the basis of the analysis presented to date. To know whether the consensus view of revolutionary change is more likely than some alternative will require that this debate be placed on a more rigorous intellectual footing—and the stakes in this debate are high enough that developing this deeper understanding warrants high analytical priority.

Rush to Information-Based Warfare Gambles with National Security
Col. Alan D. Campen, USAF (Ret.)
SIGNAL, July 1995
Col. Campen describes a situation in the United States in which "experts are concerned about the uncertainties in understanding the defensive side of information warfare. These experts equate the vulnerabilities of electronic information systems to, as John Deutch says, the potential for an 'electronic Pearl Harbor.'" Col. Campen also states that no nation is more vulnerable than the United States to electronic attacks, or, apparently, more reluctant to confront this potentially disabling weakness. The United States is suggested to be ill-prepared for an information war because the United States itself remains embarrassingly vulnerable to information attack. He also charges that a rank-, protocol-, and process-conscious military must make significant structural changes to its doctrine, organization and procedures and eliminate those echelons that contribute no added value to the flow of information. It is only by addressing these issues that the United States may continue to make its foray into the world of information warfare.

Strategic Information Warfare: A New Face of War
Roger C. Molander, Andrew S. Riddile, Peter A. Wilson

available online at: http://info.rand.org/publications/MR/MR661/MR661.html

(from the preface) "...summarizes research performed by RAND for the Office of the Assistant Secretary of Defense (Command, Communications and Intelligence). The objective of this effort was to garner perspectives on a broad range of potential national security issues related to the evolving concept of information warfare, with a particular emphasis on the defensive aspects of what is characterized in the report as 'strategic information warfare.' This report should be of special interest to those who are exploring the effect of the information revolution on warfare. It should also be of interest to those segments of the US and broader international security community that are concerned with the post-cold war evolution of military and national security strategy, especially strategy changes driven wholly or in part by the evolution of, and possible revolutions in, technology."

War in the Information Age
Army War College, Carlisle Barracks, PA
Gordon R. Sullivan, James M. Dubik
June 6, 1994
The authors of this study suggest that today we stand at what many consider the threshold of the information age—an age that has already begun to transform the conduct of warfare just as the industrial age did earlier. New weapons systems, organizations, and operational concepts will emerge, just as they did in response to industrialism. This monograph explains the governing concepts of the industrial age and how they affected the concept of war. Then it describes the concepts emerging to govern the information age and suggests ways in which these concepts may affect the conduct of war. Finally, the monograph discusses those steps that the Army is taking to position itself to exploit what are becoming the dominant military requirements to the information age: speed and precision. Specifically, the authors discuss the ways in which the Army has changed its strategic systems over the past several years so that the Army operational and tactical forces will be able to "see" a situation, decide, adapt, and act faster and more precisely than their opponent. These changes will give strategic planners, and operational and tactical commanders, a new set of information age tools to use in theater and on the battlefield. The net result: more flexibility, more versatility, faster decision making, and broader scope of weapons systems at their immediate disposal.

What is Information Warfare?
Martin C. Libicki, Center for Advanced Concepts and Technology
Institute for National Strategic Studies, National Defense University.
August 1995
This paper can be viewed online at: http://www.ndu.edu:80/ndu/inss/actpubs/act003cont.html
Overview of Command and Control Warfare (C2W), Intelligence-Based Warfare (IBW), Electronic Warfare (EW), Psychological Warfare, Hacker Warfare, Economic Information Warfare, and Cyberwarfare. Libicki asks, overall, whether information dominance is possible. He argues that although information systems are becoming

important, it does not follow that attacks on information systems are, therefore, more worthwhile.

I. SIMULATIONS

Bibliography Listing

The Day After...in the American Strategic Infrastructure (STEP ONE)
RAND Corporation
Roger C. Molander, Peter A. Wilson, Andrew S. Riddile, Michelle K. Van Cleave
June 1996
STEP ONE is the first step in a three-stage simulation created by RAND to "explore new and evolving post-Cold War international security problems, in particular in the realm of new types of strategic warfare." The participants in the simulation take on the role of advisors to a senior-level decision maker in a group deliberative process akin to a classic time-constrained "pre-meeting" in advance of a formal deliberative/decision-making meeting (such as a National Security Council meeting). The group's primary task in each step in the exercise is to finalize a document or set of materials for such a meeting. In general, several groups go through the identical exercise at the same time and compare the character and results of their deliberations at the end of individual steps or at the end of the exercise. In all three different steps (each is at a different level of decision making), the groups are presented with draft Presidential "issues and options" memos for revision and expansion, and all groups at all levels are encouraged to present, if possible, consensus recommendations on specific options that they believe the President should choose on issues put forward for decision.

Defense Information Systems Agency (DISA) Information Warfare Simulation
Home Page: http://www.disa.mil/D8/iw/iw.html
DISA is the information systems agency for DoD. This site was created to establish links to several important areas of current IW technology. As described in the introduction, "basically anything which interferes with the cognitive aspects of the command aspects of the command process or its support are fair game to us." Aspects of IW such as cultural influences and visualization using virtual reality and semiotics are to be addressed. The page and the projects it describes are still in progress.

J. TECHNOLOGY

Bibliography Listing

Information Warfare: Selected Long-range Technology Applications
W. J. Barlow and R. D. Turner, IDA Paper P-3157
Institute for Defense Analyses (IDA)
1801 N. Beauregard St.
Alexandria, Virginia 22311-1772
February 1996

IDA reviewed DoD policy and definitions relevant to Information Warfare (IW) to establish a framework for examining technology applicable to IW. As a follow-on to an earlier survey of emerging technologies in the civil sector (see below) that could have long-term influence on DoD IW activities and initiatives, IDA conducted assessments of the implications of these technologies in 12 salient applications areas. These assessments address (1) civil technology sectors that will likely influence the evolution of DoD IW capabilities, and (2) specific DoD IW application developments that could be structured to take advantage of strong technology efforts in the civil sector. Two central findings of the IDA study are that (1) availability of affordable, high-performance information-handling capabilities in the civil sector intensifies the need for new approaches to information security, and (2) civil-sector information technology can help DoD achieve new IW functional capabilities that will strengthen warfighting capabilities and enhance readiness.

Information Warfare Technologies: Survey of Selected Civil Sector Activities
W. J. Barlow, R. D. Turner, J. M. Boone, A. E. Brenner, G. L. Brown, J. L. Gerrity, W. T. Mayfield, R. D. Raines, R. S. Ross, IDA Document D-1792
Institute for Defense Analyses (IDA)
1801 N. Beauregard St.
Alexandria, Virginia 22311-1772
February 1996
At the request of the Joint Staff (J6), IDA conducted a survey of emerging technologies in the civil sector that could have long-term influence on DoD Information Warfare activities and initiatives. The survey did not include generic technologies for information systems, or other technologies applicable to sensitive areas that have low visibility in the civil sector. From over 10,000 technology/concept candidates, the survey team chose 56 technologies that are briefly described using a specified Joint Staff format that identifies technology strengths and weaknesses, potential applications, compatibility issues, technological risks, and potential limitation. In addition, the document includes an overview of information warfare activities in selected Defense Agencies and brief surveys of (1) some trends and implications of technological growth of information technology in the civil sector, and (2) some areas of concern with respect to distributed information systems.

Configurable Computing
Scientific American
John Villasenor and William H. Mangione-Smith
June 1997
This article describes computers that modify their hardware circuits as they operate. Field-programmable gate arrays (FPGAs) allow these computers to filter data rapidly. This produces a variety of results, including more complete and sharper images as well as faster comparisons between input images and stored templates. An example is made of target recognition, in which the greatest challenge is the rapid comparison of an input to

thousands of templates stored in the computer's memory. The input set of bits would represent an image made up of thousands of pixels (picture elements) being recorded on video or scanned into the computer. The target element could appear at any position within that image. A template could represent the front or side view of a specific type of vehicle. To recognize targets fast enough for military applications, a system needs to perform comparisons at the rate of several trillion operations per second, because all the pixels in the input image must be compared with all the pixels in many templates. Recognition is achieved when a certain threshold of matching is found. This kind of processing is also key for simulations of war games and other situations that require both speed and variability of processing.

The Electromagnetic Bomb—A Weapon of Electrical Mass Destruction
Carlo Kopp (homepage http://www.cs.monash.edu.au/~carlo/)
Defence Analyst, Melbourne, Australia
Available online at: http://www.cdsar.af.mil/kopp/apjemp.html
High-power electromagnetic pulse generation techniques and high-power microwave technology have matured to the point where practical E-bombs (electromagnetic bombs) are becoming technically feasible, with new applications in both strategic and tactical information warfare. The development of conventional E-bomb devices allows their use in non-nuclear confrontations. This paper discusses aspects of the technology base and weapon delivery techniques and proposes a doctrinal foundation for the use of such devices in warhead and bomb applications.

K. REFERENCE MATERIAL

Bibliography Listing

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance
Prepared by Science Applications International Corporation (SAIC), Telecommunications and Networking Systems Operation for the Joint Chiefs of Staff (J6)
July 1995
Revised version compiled and edited by National Defense University in collaboration with the Joint Staff
2nd edition, July 4, 1996
Thorough review of the organizations that have a stated role in information warfare and those that have related missions and functions. Environmental areas examined include: information infrastructure, legal environment, regulatory environment, policy environment, emerging technologies, and adversarial capabilities. This study documents extensive organizational and reference information and is suggested to be viewed as a source book on information warfare/information assurance background, stakeholders, interests, and activities. Each operational summary of an organization includes: the organization, a senior information official (current as of July 1996), points of contact,

IW/IA related missions and functions, IW/IA activities, issues, best practices, and lessons learned.

Jane's Special Report: US Information Warfare
Dr. George Stein, with contributions from Col. Richard Szafranski, USAF (Ret.)

This report provides one of the best comprehensive introductions to Information Warfare (IW) available. Stein includes a history of the information age, a conceptual overview of IW, organizational concepts (including an assessment of Joint Vision 2010 and a comparison of IW to Air and Space power), resistance to IW, suggestions and initiatives on the road to a national IW strategy, and information models for the 21st century. The concept of Information Superiority is explored, as are topics such as ethics of IW and military resistance to IW. An extensive bibliography is cited, including a special section for Government publications and laws. An acronym list and a glossary are also provided.

Information Warfare Tutorial
U.S. Army War College
available online at: http://carlisle-www.army.mil/usacsl/iw/tutorial/intro.htm
The material in this tutorial represents an unclassified version of the advanced course on Information Warfare (IW) at the U.S. Army War College. The tutorial modules consist of: an Executive Summary, How Did We Get Here?, The Threat, DoD Roles and Missions, Information Assurance, the Political Quagmire, IW Weapons, Loss of Sanctuary, the Military Perspective, Recommendations, and a Summary and Conclusions.

Jane's Defence Glossary
http://www.thomson.com/janes/public/defence/glossary/janesgloss.html
Compiled by Jane's Information Group
glossary/acronym search available at: http://www.thomson.com/cgi-bin/janes/janesrch.cgi
Comprehensive and frequently updated glossary of terms and acronyms. This database can be searched by acronym, term, field of study, and country.

Glossary: The Convoluted Terminology of Information Warfare
http://www.informatik.umu.se/~rwhit/IWGlossary.html
compiled by: Dr. Randall Whitaker
(Introduction) "This glossary contains a summary collection of some of the terminology encountered in the IW literature. The criteria for inclusion in this listing include (1) opacity to the lay audience and/or (2) crucial usage in military IW discussions. This is an excellent reference for anyone unfamiliar with the acronyms and "slang" terms of information warfare.

Information Warfare: A Working Bibliography
Compiled under the direction of Prof. Thomas C. Czerwinski
Institute for National Security Studies, National Defense University
7 August 1997
An annotated working bibliography listing the most current ideas on information-based warfare. Updated on a continuing basis, this bibliography provides insights to an extremely broad coverage of topics. It is used for background references by the Advanced Concepts Technologies, and Information Strategies Directorate in the School of Information Warfare and Strategy. Section I lists books; Section II contains monographs, proceedings, papers, reports, theses, and briefings; and Section III gives articles.

Appendix A

TERMS AND DEFINITIONS

Appendix A
TERMS AND DEFINITIONS

This glossary of terms and definitions related to information operations includes definitions contained in the following documents:

- DoD Directive S-3600.1, "Information Operations (IO)," December 9, 1996.
- Joint Pub 1-02, "Dictionary of Military and Associated Terms."
- Draft Joint Pub 3-13, "Joint Doctrine for Information Operations."[1]

Glossary From Second Draft of Joint Pub 3-13

Part II—Terms And Definitions

command and control. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02)

command and control warfare. The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare is an application of information operations in military operations and is a subset of information warfare. Also called C2W. C2W is both offensive and defensive: a. *C2-attack*—Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. *C2-protect*—Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, destroy the friendly C2 system. (Upon approval of JP 3-13, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.)

communications security. The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity materials and information. a. *cryptosecurity*—The component of communications security that results from the

---

1 Source: "Defense Information and Electronics Report," Vol. 2, No. 29, July 18, 1997.

provision of technically sound cryptosystems and their proper use. b. *transmission security*—The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. c. *emission security*—The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. *physical security*—The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons. (JP 1-02)

computer network attack. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.) (Note: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

counter-deception. Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Counter-deception does not include the intelligence function of identifying foreign deception operations. (JP 1-02)

counter-intelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (JP 1-02)

deception. Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (JP 1-02)

Defense Information Infrastructure. The shared or inter-connected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs. The Defense Information Infrastructure connects DOD mission support, command and control, and intelligence computers through voice, telecommunications, imagery, video, and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. Also called DII. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.)

defensive information operations. A process that integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counter-intelligence, electronic protect, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (Upon approval JP 3-13, this term and its definition will be included in JP 1-02.)

directed-energy warfare. Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. (JP 1-02)

electronic warfare. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. *electronic attack*—That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. *electronic protection*—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly combat capability. Also called EP. c. *electronic warfare support*—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence and electronics intelligence. (JP 1-02)

global information infrastructure. The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The global information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the global information infrastructure. Also called GII. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.)

information. a. Facts, data, or instructions in any medium or form. b. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.) (Note: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information environment. The aggregate of individuals, organizations, or systems that collect, process, or disseminate information, also included is the information (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.) (Note: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information-based processes. Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes or sub-processes which, taken together, make up a larger system or systems of processes. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.)

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.) (Note: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information superiority. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (Upon approval of JP 3-13, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.) (Note: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information system. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. (Upon approval of JP 3-13, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.) (Note: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

information warfare. Information operations conducted during time of crises or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW. (Upon approval of JP 3-13, this term and its definition will modify the existing term and its definition and will be included in JP 1-02.) (Note: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

intelligence preparation of the battlespace. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02)

military deception. Actions executed to deliberately misled adversary military decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are: a. *strategic military deception*—Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations. b. *operational military deception*—Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations. c. *tactical military deception*—Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. d. *Service military deception*—Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. e. *military deception in support of operations security (OPSEC)*—Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. (JP 1-02)

military operations other than war. Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combinations of the other instruments of national power and occur before, during, and after war. Also called MOOTW. (JP 1-02)

national information infrastructure. The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable,

wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. Also called NII. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.)

offensive information operations. The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation Also called OPSEC. (JP 1-02)

psychological operations. Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (JP 1-02)

specific information operations. Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. Also called SIO. (Upon approval of JP 3-13, this term and its definition will be included in JP 1-02.) (NOTE: This term promulgated in DODD S-3600.1 of 9 Dec 96.)

(This page is intentionally blank.)

Appendix B

TEXT OF INTERVIEWS

Appendix B
TEXT OF INTERVIEWS

DR. KEN ALLARD

President and CEO of Cyberstrategies, Inc.
July 14, 1997

Dr. Allard began by suggesting categories into which we could group the information we found. The Information Age as we know it, Allard states, is actually the second information age. The invention of the printing press revolutionized communication and made information available to a much broader group of people. It allowed mass production and distribution of information for the first time. The concept of an information revolution, therefore, is not historically unprecedented. Allard continued the discussion with a description of what he considers to be the background to examining the more recent evolution into a new Information Age:

The natures of changes that have been occurring since the 1980s have been broad-based. The computer chip has revolutionized many areas of our lives, with much of the observable difference occurring in three major areas. Computers themselves are one area, and the difference between a computer in the 1980s and a computer today is amazing. Although an ***Apple IIGS*** was perfectly capable of meeting the needs of the average person 10–15 years ago, to think of using a machine like that now is amusing. Communications is another area of dynamic change with much of the change in this area relating to satellite-based linkages between computers—the effect of which is the communications revolution we see on the phone, on the computer, and even on television. Television is the third area, meaning the development of advanced imaging capability, creating better, sharper images faster than ever before. These technological advances alone provide fundamental alterations in the nature of human interactions. And looking at these three in addition to the creation of the Internet, the effect of mass media like CNN, and natural science advances in molecular biology, chemistry, and physics is staggering. It is the synergistic effect of all of these elements that people are calling the Revolution in Military Affairs.

It seems that in many situations people are jumping up and saying that in the future we will have wars without conflict. All we will have to do, for example, is take down our enemy's stock market. It seems to Allard, however, that suggestions like these are not at all helpful. What you have to parlay that mindset against is the following: the only things that have not changed in any of this are "the nature of man" and what Allard calls the "permanently operating factors" of friction and war. History is incredibly important in instances such as these because "as soon as you say something is unprecedented, watch out." Allard feels history does have lessons to teach but does not suggest that history repeats itself. "Anyone who thinks that history repeats itself," he declares, "has never read history." There are, however, some "bold problems here," and this is a combination of old and new. "We are still dealing with the potential for human conflict, and when push comes to shove, if I can take down your stock market fine, but that will in no way, shape, or form stop me from knifing you if I possibly think I can. Things get reduced to their essence very quickly."

The fundamental question is, what is the application of these revolutions to the tools of war? On one hand, there are people who say that nothing has changed at all and what we must remember is that more vulnerabilities than capabilities exist in this field. At the other extreme, some people believe we will end up with "push-button war." Allard finds both of these extremes to be fallacies.

Set forth below are Allard's response to the specific questions posed by the study.

Question 1

IDA: What do you consider to be the major issues in the broad field of Information Operations, Information Warfare, Information Assurance?

KA: *One major issue that needs to be looked at is the question of the infrastructure. This is being looked at right now by various Presidential commissions. As a nation we have fought on and off for 200-odd years over what the Government can and cannot do. Currently we are asking ourselves "What is Government and what is private sector and who is responsible for what?" We are properly taking a look at these areas.*

Question 2

IDA: Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level? By the military? In the civil sector?

KA: *In the military we are not taking a good look at how the military infrastructure has to change. This is the fundamental question and issue.* (This is addressed in the final chapter of his book.) *By DISA's estimate, there are between 5,000–9,000 legacy systems in operation, which it would cost huge amounts of money to upgrade or replace.*

Allard's implied suggestion is that we should be reorganizing the hierarchy of the military echelon before we put money into replacing or upgrading systems, which might be scrapped after a reorganization. *"We have to answer the question of, 'What does the DoD do to prepare for an information-based environment?' The answer to this question, whatever it might be, will fundamentally alter the nature of human conflict."*

Allard cites as an example the fact that the QDR does not address this as an issue or as a problem. We have an interoperability problem, and it's getting people killed—the Blackhawk helicopter shootdown in Northern Iraq, for example. *"This situation was basically a problem with the identification of friend and foe, and we sacrificed 26 lives to the altar of interoperability."* Apart from the human interest of this, we have a problem getting information down to the lowest level. Therefore, it is an infrastructure issue in terms of redundant systems; it is an organizational issue in terms of *"what are those organizations doing and is it still appropriate?"* and most fundamentally, what is the nature of leadership? We watch the question broaden from specific systems to organization to the fundamental philosophy behind the actions. How does the commander command? These issues are inexorably linked.

Question 3

IDA: How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention?

In the area of offensive IW, Allard believes that there must be some kind of capability for us to do what a hacker can and does do every day. The fundamental question here is *"if I'm more vulnerable to this than the other guy is, should I be the first one to start it?"* We have to consider, as in the case of nuclear deterrence theory, the downstream effects of waging an offensive information warfare campaign. Suggesting, in a war or wargame situation, that you "just take out their economic system" is ridiculous when you consider the consequences to the rest of the world. This question is, in Allard's eyes, *"the unanswered question."* Gaming and simulation could be very useful in addressing this question despite its almost philosophical nature. There is a very fundamental question to

be addressed, however, that resides at the very core of the issue, and that is, "Is offense good or bad?"

KA: *On the defensive side, we have not yet begun to fight. I don't think anyone beyond maybe the Air Force has begun to think critically enough about this. We have an obligation to secure our warfighting systems insofar as we can. The baseline thing that I would really like to see more work on is* [that] *we have to develop a calculus on our defensive Information Warfare. We need to figure out ways to calibrate and protect information. How does this affect me if I lose it? And how is that information of value to me? Am I better off proliferating it, should I superencrypt it? As for right now, that's where I would put the emphasis.*

We experienced a post-war euphoria after the Gulf War, not thinking about the fact that Sadaam Hussein didn't send in a force of hackers to attack us, and, if he had, things might have gone differently.

We have not paid enough philosophical attention to the offensive side of the issue, and on the defensive side, we have not yet begun to fight.

KA: *I just keep coming back to this one issue, though, and that is, I'm not prepared to think about offense or defense if I don't understand the nature of my own system. If you don't understand it, you can neither improve nor secure it.*

Just because we have this vastly decentralized system doesn't mean that no one will be able to attack it. Self-induced information warfare doesn't improve the situation. We also cannot afford the systems we have right now, which means we don't have extra money to revamp these systems.

The linkage of these issues again is systems to organization to philosophy of leadership.

Question 4

IDA: The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in the Government for dealing with this issue at the national level?

KA: *On the evolution of information technologies, that is something that Government cannot even begin to do. They can barely keep pace with what is happening in the*

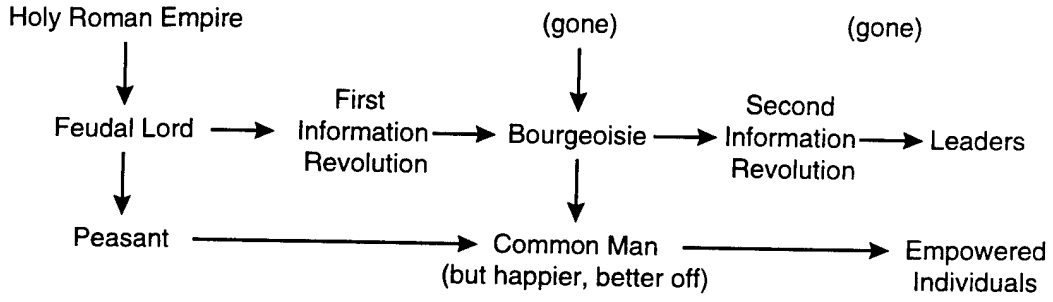
commercial world to import patents and technologies for use in the Government. I really see them as playing very much a second fiddle to what is happening in the commercial arena in terms of creating the technology, using it, exploiting it. The most Government can do is impose a very few—a very few—fundamental choices because most of this will be taken care of in ways that the Government cannot deal with. The basis of all of this development will be money. This kind of change goes beyond the Department of Defense, beyond the Government, and beyond the Nationstate because the bottom line is that we need to be able to do commerce more efficiently.

So what is the role of Government? Diminimus. Get the hell out of the way.

What makes you think you can trust the Government? What makes us think that NSA has the right to monitor our conversations? Well, they say, someone has to protect us from drugs. Aren't they doing a wonderful job of that?

IDA: What about the fact that there are things on the net that aren't necessarily harmful if taken alone, like the blueprints of devices or of locations, but if taken in conjunction with other things, like materials to make weapons or the desire to destroy a particular type of location, are extremely harmful? Shouldn't there be some element of Government control over what is available on the Internet?

KA: *Remember your Aristotle. Everything in moderation. I'm not saying it can't say some things. One of the things it will have to answer is who is in charge if something horrible happens. Basically Government is designed to provide for the common defense and promote the general welfare. Now, what is the role of the Government in helping to* promote *this new information age society? Education and defense are two of the things that represent center of mass on those things in which Government is considered to have some amount of competency in. Not much. I'm not saying that the Government is irrelevant—far be it from me to say that—but I'm saying that its ability to influence this information age strikes me as being a lot less significant than what it could do in the industrial age, if you want to use a Tofflerism. Historically, you might trace the shift of power like this:*



In short, the effect of this second information revolution will be most evident in the power shift toward the individual empowered by information. Government control is a feature of the industrial age.

KA: *When it comes to technological development, rank and age are in inverse proportion to competence.*

Question 5

IDA: What obstacles do you see to developing an effective national "cyber defense," and what should be done to overcome them?

KA: *One of the most fundamental problems to a national cyberdefense is interoperability. There are in-built differences that are perpetuated in systems. This brings us back to an argument on standards: we need a rigid and inflexible series of standards, commercially based and enforced.*

The two obstacles, therefore, are an awareness problem and a standards problem.

We're not even sure we're asking the right questions yet! We have to reconceptualize civil defense in entirely new terms.

In the 19th century, our great public work was to put cannons at the mouths to harbors. Go down to Fort Monroe at Hampton Roads and you'll see evidence of this. What do we do in the 20th century? We create the DEW line, the Defense Early Warning system, which was a great electronic fence, backed up by missiles. This was civil defense at that time. For the 21st century, that degree of public work will have to be done somehow. That is a legitimate function of Government and will be equally fundamental as the 19th and 20th century.

Question 6

IDA: How should the United States focus its resources to address the necessary elements of change and use these elements to its advantage as well as defend itself in the information age?

KA: *Point one: the Information Age is affecting all of our institutions. Some more than others, but it is affecting them all. This information technology will change organizations and we will have to accept the fact that we need to fundamentally realign technology and institutions. More asymmetric vulnerabilities will be created due to more communication and access to information and, from that, defenses will have to arise, but they will result from a problem that someone will nail, the defense will fail, and we will try to fix it again. If you choose to call it an "electronic Pearl Harbor" that's fine, but no matter what you call it there will be problems. Hindsight will be our defensive impetus.*

IDA: Is there a way to make this *not* a defensive issue?

KA: *We need to focus people on the idea of having a damage-limiting strategy. Sure, if you shut down my system I will hate it, but if I have a reachback mechanism, I will at least know where I was yesterday.*

The answer to that question, however, is hindsight now applied. We will need a demonstration shot, and then we will defend ourselves.

Question 7

IDA: How should we approach the use of IW concepts and strategies with our allies to achieve an ordered response to crisis?

KA: *In terms of working in groups, one finds that virus is spreading and all the downfalls of free computing are directly analogous to the AIDS virus. When you have free computing and one interface strand, you also have all the problems that go with it. So, again, we have to have commercial guidelines/standards. Now how much of this information do you share with the allies? This is a situation-dependent issue.*

Point one: there is a general consciousness-raising that has to occur; point two: there also needs to be an enthusiasm for the abilities of the commercial market.

As for sharing information, we are much more open than most countries. The British, for example, are very unwilling to share information. It is imperative to consider the "shelf-life" of information, and most are talking in terms of cans; we're talking perishables.

An ordered response to crises? I don't think so. It will be enough if we can at least create an imbedded series of defenses, if we can realize that the refresh rate on information is such that you can't keep it secret for as long as in the past, and if we can create commercially based standards. We must begin at the conceptual level first, both within the Department of Defense and with the allies.

Question 8

IDA: What impact will the evolution of information technologies have on preventing and/or resolving conflicts with non-nation state actors (e.g., hackers, etc.)?

Allard refers to the piece he wrote in the *Washington Quarterly* called "Agenda for Cyberwar" in which he asserts that information is not inherently advantageous to anyone; it is, if nothing else, a leveling influence. "*Information will be in the 21st century what the machine gun was in the 20th.*" Whoever turns the "observe-orient-decide-act" circle the fastest will dominate the battlespace in the 21st century.

It will be increasingly difficult to distinguish state and non-state actors. One suggestion to monitor people's actions is licensing computers so, like an automobile license plate identifies you on the road, a computer can be identified when cruising the information superhighway. A computer has the potential, like a car, for great benefit and great harm. We have accepted the need to identify individuals on our physical roads. Are we willing to do this on our cyber-road? To what extent do you really want to guarantee anonymity? This issue cannot be resolved, however, until we reach a degree of international consensus that is not there right now. International consensus is necessary because there are no physical boundaries.

Question 9

IDA: What prioritization of actions would you recommend? Where do we focus attention first and where do we go from there?

KA: *Prioritization of things to be done:*

- *Review the results of the PCCIP. The idea of looking at the National Information Infrastructure is very good, and once we have information regarding this we should have a decent outline of the problem.*
- *Pin the role on someone. We have to have someone or something to deal with these issues, and the second step in this process is to determine who that should be.*
- *Specific to the DoD, we must figure out how to rationalize our specific system. This includes how to defend it and how to modernize it.*
  - *Make a hit-list of systems to be shut down because we can't afford all that's out there, we are facing a year 2000 problem anyway, and we are now dealing with the heightened threat of INFOSEC.*
- *When we examine the character of future systems, we must include these criteria:*
  - *Interoperability—No more system upgrades that don't accommodate older models. No more "parts" that don't work together.*
  - *Security—We must have a way to secure information, whether that be through encryption or intranets or any other option.*
  - *Commercial—Products used in DoD must be COTS (commercial-off-the-shelf) products so the DoD can stay current with technology. We do not have the time to let engineers and computer people try to continue to develop separate technology for the DoD. The commercial products can be used and modified to suit our needs. This allows our people to be working on more important issues, saves us money, and provides more opportunity for interoperability. We can easily build in financial incentives so businesses will spend time developing systems for the DoD.*

(This page is intentionally blank.)

ALAN D. CAMPEN

Contributing Edito,r *SIGNAL* Magazine
Manager, AFCEA International Press
Adjunct Professor, School of Information Warfare and Strategy, National Defense University (NDU).
July 1997

AC: *The structure of your questions presumes that IW is a major problem and we need to find a structured approach to solving it. I have a different view.*

The Information Age, just as the Industrial Age, brings issues with which humanity has never before dealt with. The difference is that the changes from the Industrial Revolution evolved slowly over decades; change was linear, allowing orderly adaptation, and results were reasonably predictable. Each generation was born, lived, and died in the same culture. This era is best studied by historians.

The Information Age, on the other hand, is shaped by rapid, non-linear and unpredictable change, posing problems more rapidly than can be dealt with by our culture and its processes for dealing with change. The change is debated, not by historians, but by journalists and futurists. Nobody knows what the changes portend. Prediction is impossible. History is useless.

There is no immediate crisis that must be dealt with, shaped, or controlled by any government. The Singapores and the Chinas will try, and they will fail. This revolution cannot be managed—only experienced and endured.

Travel in cyberspace will become safer only when the traveler demands it be made safer. Not before. The laws of cyberspace will evolve gradually, in response to challenge, just as they did in the industrial age. Ethics and codes of behavior will evolve, but not always in the proper direction. Example, the motorcar has become a weapon on the roadways in Fairfax County—hardly a hopeful sign that humanity will deal responsibly with its new found electronic capabilities.

Having said that, here are my answers.

Question 1

IDA: What do you consider to be the major issues in the broad field of Information Operations, Information Warfare, Information Assurance?

AC: *One major issue is that the subject of IW/IO/IA will be both over- and under-emphasized.*

Those overreacting are [of] *the "Electronic Pearl Harbor" school who assert that a nation can be brought to its heels solely by an assault on its information infrastructure, and, therefore, defense of the NII is a Federal responsibility. They will give short shrift to the far more real threats from terrorists with bombs and rogue states with cheap cruise missiles tipped with WMDs. To them I say, IW is just another and comparatively (to weapons of mass destruction) unimportant weapon.*

Those under-reacting to an IW threat are a problem because there will be no consumer demand for simple and reasonable security measures to protect the NII against all measures of vulnerabilities ranging from ankle-biters to serious and costly attacks. In this school are the people who want to "outsource" the whole national defense mission, starting with contracting out all software development to the lowest bidder. (Note the current papers on the Internet by Mary Fitzgerald which show that Russian and Ukranians leaders are worried about the same thing.)

A second issue is that the U.S. military will construct a new doctrine based on the assumption that it can guarantee information dominance on a hostile battlefield, against opponents who can arm themselves at Radio Shack. I say the best the U.S. military can hope for is "Information Equality."

A third issue is the outright hostility and lack of trust than inhibits any possibility of a cooperative nationwide effort to reducing vulnerabilities of electronic systems to malicious attack. Industry can't trust each other in the intense competitive environment, and laws would not permit them to cooperate even if so inclined.

Question 2

IDA: Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level? By the military? In the civil sector?

AC: *It all depends. If you are of the Electronic Pearl Harbor school, the answer is no. If you think we are sitting in a 20-year window of opportunity, while China gathers*

strength, then the slow progress is acceptable. The question is academic. Without a "smoking gun," the American public won't support aggressive action in any event. The important point here is that any potential opponent is also operating under the same constraints of unpredictability.

The military is working the problem as best it can, but what few additional dollars that might be made available will go for platforms and weapons, not information security. As I say in my lectures, the DoD talks network-centric, but purchases platform-centric.

The civil sector is barely aware of information security, wouldn't understand it if it were aware, and would never agree on spending money for a solution in any event. No smoking gun!

Question 3

IDA: How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention?

AC: *I wouldn't! A dynamic president and a clear national emergency might lead the nation in some general direction. Until and unless there is some national emergency, nothing will happen. We are a reactive nation. Always have been, always will be.*

Question 4

IDA: The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in the Government for dealing with this issue at the national level?

AC: *Many Government agencies have responsibilities, mainly because of an inherited tradition in the analog communications age, and also because nobody but the Federal Government can perform them. The FCC is an example of traditional responsibilities for telecommunications. The FBI, Treasury, and Secret Service all have traditional responsibilities for secure telecommunications. The digital age just adds a new dimension.*

The DoD is responsible for national defense, but are we sure that threats to the NII are a threat to national security, or are they threats to individuals, companies, privacy, etc.?

The NII is new and presents issues with no precedent. The NII is a multi-organizational private sector monster, where once we had the single Bell system. Short of a declared national emergency, DoD has no authority over the NII. Nor does any Federal agency.

It seems to me that the Government role in defending the NII can be summed up by saying it can do whatever is left over, after the owners and users have patched up every problem they can discover and correct and whatever the courts decide from the law suits that will follow any failure in the NII. History will chart the course.

Martin Libicki best describes the situation this way:

Chemical plant blows up and destroys half of Pittsburgh.

1. *Cause was missile from Cuba. Clearly Federal responsibility to defend.*
2. *Cause was rifle fire from terrorist sniper. Not Federal fault and probably not owner fault either because vulnerability is not due to lack of due diligence against predictable threat.*
3. *Cause was terrorists who penetrated facility and set off bomb. Not Federal fault, but probably owner fault for not having better security system. Lack of due diligence.*
4. *Cause was lightening. Act of nature. Nobody at fault.*

Libicki example shows danger of calling this information "war."

The information age brings added risks to those who depend on unreliable systems and thus willfully expose themselves to danger and loss. The owners and operators of information systems must act to protect themselves against law suits from customers.

The Federal Government will not be a major player in defending the NII because it lacks authority and trust. Some laws might be changed to give the DoD better oversight of the NII, but what happens when it becomes the GII? The Federal role ultimately will be limited to these:

- *Focused intelligence and warning to the private sector.*
- *The same law enforcement duties they have today.*
- *Focused R&D on defenses against malicious attacks.*
- *Perhaps some security standards.*
- *A nationwide attack detection, reporting, and restoration system.*

- *Possibly some Federally operated "break-points" where switches can disable connectivity.*
- *Education, education, education. Until the public cares, little will happen.*

Question 5

IDA: What obstacles do you see to developing an effective national "cyber defense," and what should be done to overcome them?

AC: *The obstacles are lack of consensus that there is a threat or need for any corrective actions. The obstacle is lack of demonstrated need. There is no clear and present danger. There is only a vague and ambiguous potential. We can do nothing to overcome this. Events, or lack of them, will shape the future.*

Question 6

IDA: How should the United States focus its resources to address the necessary elements of change and use these elements to its advantage as well as defend itself in the information age?

AC: *Let's wait and see what the Commission comes up with.*

Question 7

IDA: How should we approach the use of IW concepts and strategies with our allies to achieve an ordered response to crisis?

AC: *There won't be any ordered response to IW. Other nations will or will not cooperate with the U.S. on this as they do or don't on any other security issue.*

The military in UK, Canada, Australia, etc., will probably cooperate with our military on improvements in securing military information systems. To the extent we use the same technology, we share the same vulnerabilities and potential solutions.

Question 8

IDA: What impact will the evolution of information technologies have on preventing and/or resolving conflicts with non-nation state actors (e.g., hackers, etc.)?

AC: *Can't respond because you have lumped too many disparate "actors" into one category. Hackers, crackers, thugs, criminals, terrorists all have different objectives and*

motivations. Each will use, or not use, information technology if its best satisfies the goal. Obviously new information technology is giving law enforcement the fits because encryption will dry up a good source. Information technology makes crime and theft much less risky, easier, and more profitable. I doubt that terrorists care much about it as a weapon unless an attack will land [them] *on the front page or the evening news.*

Question 9

IDA: What prioritization of actions would you recommend? Where do we focus attention first and where do we go from there?

AC: *Let's see if we can improve the security of our own NII and the tactical military systems that hang onto the ends of it. That's quite enough for now, thank you. We must not end up being the most vulnerable nation in the world to the technology of our own choice—which is precisely where we are headed now.*

In theory, the world might eventually rest in peace if everyone is using the exact same interconnected information technology to conduct its internal and external affairs. Then any disruption to any of these global systems will be unacceptable because of the unpredictable domino effect.

The notion of national sovereignty will fade because it will be unenforceable. Governments will be obliged to find new ways to govern when all the normal tools fade under encryption.

Frankly I doubt we will plan for this revolution any better than we did the industrial revolution.

Be sure and see the excellent Delphi on IW done at the NPS several years back. It can be found at http://stl.nps.navy.mil/~c4ipro/thesis.html.

JAMES R. GRAY

Avenue Technologies, Inc.

Question 1

IDA: What do you consider to be the major issues in the broad field of Information Operations, Information Warfare, Information Assurance?

JG: *The first major issue is a lack of a coherent national information policy. The mark of entry into the information age seems to be having a home page or web site. Yet without a coherent information policy, this is, at best, a dangerous fad, and at worst, a threat to national security. Dangerous because so many organizations have created these sites with only a cursory understanding of what should or, more importantly, should* not *be made available on them. Examination of a large number of these sites from an intelligence-gathering perspective can be very revealing, especially since we choose, as a nation, not to allow false information to be posted on Government sites. For example, the "Sunshine Law" mandates a great deal of information about the operation of nuclear power plants be made available to the public. The Department of Energy's answer to this act was to create home pages for each of the 109 commercial nuclear facilities in the United States. These sites each include detailed site-specific (down to blueprints) information on the physical layout of the plant. This information, when cross-referenced with information from other web sites (e.g., telephone book and address locator sites) could empower an adversary with sufficient information to attack (using physical and "cyber" means) that site, its leadership, and the surrounding community. To deal with problems such as these, we have to first identify who is responsible for them. When we presented a specific and detailed version of this general scenario to the NRC* [Nuclear Regulatory Commission], *they told us "It's not our problem." Since the scenario did not deal specifically and solely with the potential release of fissionable materials, the NRC felt it did not have the regulatory responsibility to deal with it. Within the now narrow confines of their physically defined area of responsibility, the NRC is not agile enough to either understand the emerging problems, or to deal with them.*

This brings up the second major issue: The modern "information age" has changed the world profoundly, but our institutions have not adjusted quickly enough to either fully understand the problem, or to deal with it. Although the free flow of information

empowers those who do good work, it also empowers "bad actors." We have to act upon the cold fact that there are many organizations, and even individuals who, if they had the means, would strike out at us. The type of information we are making available to the entire world may provide the very key to successful attacks on what we have become used to thinking of as "Fortress America." In the example above, the nuclear power plant is a tempting target because targeting-level information has been made available to the entire world on the Internet, and nobody is technically in charge of defending it, not the DoD, not the NRC, not local, state or national law enforcement agencies. In Cliff Stoll's book, The Cuckoo's Egg, *his hunt for computer hackers is frustrated by every Government and law enforcement organization with the catch-all phrase: "That's not my bailiwick." We continue to bound our thought processes, and define our areas of responsibilities, by the rules of the physical world—and it just doesn't work. The boundaries of responsibility for public information must be reviewed. When we discover these new types of problems, we must act quickly to make it somebody's "bailiwick."*

One of the realities of the new information age is the rush to put everything on the web. As I mentioned earlier, we lack a coherent national policy in what to put, and what not to put on the web. A first step to dealing with this problem is to learn to ask ourselves not just what the gain might be if we were to put something on the Internet, [but also] *we must ask ourselves "what's the risk?" We must teach ourselves to think of such concepts as "public privacy," that is, we must identify information which, although our citizens might need access to it, the rest of the world does not. This information includes, but is not restricted to, information that reveals potential vulnerabilities about our critical national infrastructure. As a second step, Government at all levels needs to become educated on the depth of the problems that unbridled access to information and information-dependent systems can create for their constituents. To neglect this issue is an abrogation of Governmental responsibility in the new information age. Protecting your computer systems with fire walls does no good at all if an information-age terrorist (one who knows how your power and communications are delivered because he found your local power and telephone companies' web sites) simply turns off all your power and telephones.*

In short, I believe the main issues are:

a. *A lack of a coherent national information policy.*

b. *The failure of our institutions to fully understand the problem, and to adjust to handle it.*

c. *A rush to put everything on the web without adequate understanding of the risks of providing access to this information to the world. Just because we can put information on the web doesn't mean we should.*

d. *A failure to modify information-related policies and laws to protect "public privacy."*

Question 2

IDA: Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level? By the military? In the civil sector?

JG: *No.* (See above.)

Question 3

IDA: How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention?

JG: *First, we need to analyze our vulnerabilities as others see them, not just as we wish they were. If, as most of us in the business feel, our biggest vulnerability is the finance system, then that becomes a national strategic concern, not just a "commercial issue." If telecommunications, power, water, etc., are critical issues from a national strategic perspective, then we must change how we think of strategic defense to incorporate protection of these national infrastructure elements. As I mentioned above, someone needs to be in charge. Because of the nature of the threat, that someone cannot be a consortium of disparate individuals who have to check with someone else before acting on threat information. The "someone" in this case needs to be a national center, empowered and trusted by both Government and industry alike. This center must be able to detect attacks and stop them. It must first and foremost limit damage, then identify the attacker(s) and finally alert the appropriate agencies to either pursue or attack the attacker(s). This is not just a DoD problem! It's not primarily NSA's job, since they are not operators. It's not the individual Services' job because they do not have the span of authority to protect the nation. The center must be national, with DoD input, but run by some other the Federal Government department, perhaps even a new one created to deal with information.*

Secondly, we need to treat information as a national asset. Information which is potentially dangerous to the citizens of the United States or its interests needs to be assiduously protected. We need to develop technologies that better protect our

information-dependent infrastructure elements, and our competitive advantage in the global marketplace.

Bottom Line: We must reinvent national defense for the information age. We must identify and quantify our information-related vulnerabilities, and craft a national strategy to protect them. This means establishing a national IW center run by the Executive with representation from DoD, State, Justice, CIA, NSA, DIA, and commercial interests.

Question 4

IDA: The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in the Government for dealing with this issue at the national level?

JG: (See above.) *Since this problem is bigger that the constitutionally defined limits of power for the military, I believe most of us would be more comfortable with another department, or perhaps the Executive itself, running the center that is responsible for it.*

From the DoD perspective, although they currently are responsible for WMD [weapons of mass destruction] *issues, perhaps it's time to redefine the role of STRATCOM* [Strategic Command]. *After all, we are talking about the new concept of strategic survival, so perhaps DoD's focal point needs to be STRATCOM. I think I would even morph the name a little to Information-STRATCOM, or just INFOCOM. But giving responsibility for this area of conflict, which will soon be an even more important arena of warfare, to a standing CINC will go a long way toward resolving the non-productive struggles in the DoD about who's in charge.*

Question 5

IDA: What obstacles do you see to developing an effective national "cyber defense," and what should be done to overcome them?

JG: *The primary obstacles are rooted in policy and procedure. Whose job is it? Is it legal? How do we modify roles and responsibilities to be consistent with the realities we face today? And how do we answer these questions in real time?*

From the private sector perspective, most organizations are reluctant to join in a national effort to protect the "infosphere" for selfish (and short-sighted) reasons. Banks do not

want to admit to the enormity of the problem because (1) they see automation as away to decrease costs and increase profits—any increase in PC banking or ATMs will help their bottom lines—and (2) banks operate on public faith. They feel a full disclosure of how much they [could] *lose would cause a loss of that faith.*

But perhaps the most difficult obstacle to overcome is our problem with all of the disparate perceptions of the problem. National Government agencies and departments are struggling with rules, laws, and regulations that divide responsibilities for action based upon a physical world paradigm. They are trying to define their roles and responsibilities upon concepts that do not apply in the cyber world.

For example: If a crime is committed in the United States, you first need to determine if is a state or Federal issue. Then you can assign someone to investigate. But if it is terrorism, then the FBI is in charge—unless it's from overseas, then the CIA is in charge—unless it's being planned by a U.S. citizen, then the FBI is in charge again. By the time we determine there is activity, and what the activity is, and assign responsibility for action, the damage is done. The compression of time with information technology has collapsed our decision cycle, just as we collapsed Saddam's decision cycle during the Gulf War. We no longer have the luxury of assigning the right "second wave" organization to handle the problem. What is needed is an entirely new organization that can detect activity, correlate it, report it, and take necessary action to limit damage. First step: Identify potentially damaging activity. Second step: Isolate that activity and limit damage. Third step: attempt to discover where the activity originated. Final step: Determine what action is necessary and assign someone to pursue that action. Just as the first rule in an aircraft emergency [is] *maintain aircraft control. Everything else comes later.*

Question 6

IDA: How should the United States focus its resources to address the necessary elements of change and use these elements to its advantage as well as defend itself in the information age?

JG: *From a DoD perspective, I find it very troubling that each Service has created an IW center primarily manned by contractors. The argument is that they can't keep trained operators in the Service. That's ridiculous. Pay incentives, offer college, offer training in exchange for extended enlistments. There are all sorts of alternatives. The real problem with today's arrangement may come when a contractor loses a contract—all of a sudden*

you have just created a whole host of the most dangerous IW adversary, a disenfranchised former insider. Each Service should be directed to maintain a uniformed capability in IW. After all, these are the new "front line troops." We cannot afford to have them all be mercenaries.

From a civilian commercial perspective, if they don't participate, we simply identify their vulnerabilities for them. As we begin the development of our Information Defense, we won't need their detailed participation, simply their understanding that they are part of the national matrix that must be protected. Second, we put a non-DoD department in charge of the effort, although DoD has a role. Third, we educate our leaders about the dangers of worldwide unbridled access to critical U.S. information. Fourth, we quantify the problem and develop strategies to solve the problems.

Question 7

IDA: How should we approach the use of IW concepts and strategies with our allies to achieve an ordered response to crisis?

JG: *We have to keep our allies informed, especially in* fora *such as NATO. Inviting close ally participation in high-level games (e.g., EVIDENT SURPRISE) would be an excellent first step. Roll IW/IO/IA issues into NATO exercises and training. The Warrior Prep Center at Einsedlerhof is a great center for beginning this training.*

Question 8

IDA: What impact will the evolution of information technologies have on preventing and/or resolving conflicts with non-nation state actors (e.g., hackers, etc.)?

JG: *Focused efforts on identifying attacks and cutting off access to the attacker(s) will help limit damage. Retaliation will probably be difficult, if not impossible, and perhaps should not even be a policy goal. Simply denying success to "hackers" will both discourage the casual "hacker" and strengthen our defenses against more determined attackers. Technology will play a role, but so will psychology, "man-in-the-loop" detection systems and "cyber HUMINT."*

Question 9

IDA: What prioritization of actions would you recommend? Where do we focus attention first and where do we go from there?

JG: *First establish a national IW center as discussed above.*

Second, consider establishing a Department of Information with a Secretary in the Cabinet. Information is arguably a more valuable strategic resource to this nation today than transportation. In fact, with the emergence of information as a pre-eminent building block of transportation, energy, commerce, and justice in our society, it may have become the most valuable strategic resource. With that in mind, perhaps this is the true first step we need to take: establish a Department of Information.

Third, it's time to bring the debate about the cons of the modern information age to the forefront. Issues such as information vulnerability, privacy, and unbridled access to information must be examined in light of technology advances that rapidly strip away all our privacy. Should we be more concerned about censorship or the revelation of potentially strategic-value information about infrastructure vulnerabilities? Is the question about "Net Nanny" programs or worldwide accessibility to your tax returns, private health records, earning information, and social security information? Technology should be used to serve our societal objectives. And that means we need to take a new look at those objectives.

Finally, we need to embark on a catch-up education program. It's difficult to get technologically astute policy decisions from decision makers who can't program a VCR. The world is different. Conflict in the modern information age will not likely respect the Geneva Conventions. As with information age vandalism, modern information age warfare will most likely be indiscriminate, without concern about "collateral damage." As in the recent attack on George Mason University, the loss of research data by a few graduate students was of no concern to the hackers. Their apparent goal was to punish the University, so they attacked its computer systems. That a few students were attacked along the way was not important to the attackers.

(This page is intentionally blank.)

DANIEL KUEHL

School of Information Warfare and Strategy
National Defense University (NDU)
September 4, 1997

Question 1

IDA: What do you consider to be the major issues in the broad field of Information Operations, Information Warfare, Information Assurance?

DK: *I think there are four critical issues here. One is the emergence of cyberspace as an operational environment. In some ways, this dates back to WWII (I did my doctoral dissertation on the USAF and Electronic Warfare after WWII, which was—in my concept—the first war in cyberspace). But, of course, the emergence of the computer revolution has been the key here. Next is the increasing omni-linking of the global electronic digital world. Third, is the need to differentiate between the two lunatic fringes: "the sky is falling, there's a hacker terrorist behind every hard drive," and the "there's nothing new here, it's all old wine in fancy new bottles"—and focus on the real and substantial changes that are taking place because of the information revolution. Finally what is* force *in the information age? Does* war *require bombs and blood, and how might a nation react to something that is very harmful but not explosive?*

Question 2

IDA: Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level? By the military? In the civil sector?

DK: *These issues are not being addressed at the national lever, although the formation of the President's Commission on Critical Infrastructure Protection is a good start. The military is taking the most proactive look at IW, but it is increasingly narrowly focused on "info warfare" instead of "info age national security."*

Question 3

IDA: How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention?

DK: *Somehow we must make a more effective argument that IW is not just about electrons and computers, but also involves the mind and wetware. PSYOPS may not be*

anything new, but the technologies of the info age open some tremendous—and perhaps frightening—possibilities and vulnerabilities.

Question 4

IDA: The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in the Government for dealing with this issue at the national level?

DK: *No one at present can be said to "have the lead," and perhaps this is as it should be. We do need, however, some form of coordinating body that brings the players together and provides a forum for discussion and cooperation. The key missing piece is national-level Governmental leadership. The President must take the lead here, because all the different players will never voluntarily come together without strong and forceful leadership at the top. We do need a national info policy.*

Question 5

IDA: What obstacles do you see to developing an effective national "cyber defense," and what should be done to overcome them?

DK: *Two big issues: "What's the threat?" and "Watch out for Big Brother!" The defense community is driven by identifiable threats that can be quantified and modeled, and neither works for IW. The privacy issue is big, and our electronic civil liberties crowd is focused on the wrong threat—it's not "Big Brother" but the commercial world that wants our personnel for commercial reasons.*

Question 6

IDA: How should the United States focus its resources to address the necessary elements of change and use these elements to its advantage as well as defend itself in the information age?

DK: *The information age can be seen as a combination of numerous necessary elements, including technology, the human factor, process, and policy. It is vital to our understanding of and response to this new era that we address all necessary changes in both ideology and practice. How should we, as a nation, focus our resources to address the necessary elements of change and use these elements to our advantage as well as defend ourselves in the information age?*

IDA: Defense seems a monumental task, and is, as such, the subject of the current President's Commission on Critical Information Infrastructure Protection. The suggestion by the Commission is that the fix to this is obviously a public and private partnership that tackles the issues of information assurance, especially Indications and Warning (called "operational warning" by one of the panels) on a sector-by-sector basis. Each "critical" industry and subsequent type of information infrastructure, has its own needs and must be addressed within the context of its specific capabilities and vulnerabilities. With that framework in mind, however, what suggestions might be added?

DK: *I fully agree with the public and private partnership as suggested by the PCCIP format. Now, how do we bring these players together when the private sector is increasingly suspicious of the public sector—suspicious of both its motives and its efficiency.*

Question 7

IDA: How should we approach the use of IW concepts and strategies with our allies to achieve an ordered response to crisis?

DK: *We need to get out of the "green door" mentality as much as possible, because far too much is too highly classified. Just two years ago, for example, it was highly classified to link computers with IW. Get real!*

Question 8

IDA: What impact will the evolution of information technologies have on preventing and/or resolving conflicts with non-nation state actors (e.g., hackers, etc.)?

DK: [Not prepared to address at this time.]

Question 9

IDA: What prioritization of actions would you recommend? Where do we focus attention first and where do we go from there?

DK: *The absolute number one priority is to continue to develop the education of the info-knowledgeable leaders, both military and civilian, for the world of the 21st century. Without education, we won't get anywhere. The next priority is to spur further coalescence of the public and private sectors to see this as a shared responsibility.*

(This page is intentionally blank.)

JOHN E. McCLURG

Federal Bureau of Investigation
July 22, 1997

In light of John McClurg's position in the FBI, the discussion during the interview was very general in nature. This report serves to describe the organizations and positions in the FBI related to IW and Infrastructure Protection, as well as to describe Mr. McClurg's position and views on some of the issues raised by the interview questions.

Mr. McClurg is a supervisory special agent with the FBI who serves as one of twelve members of the Infrastructure Protection Task Force (IPTF). The task force was created on July 15, 1996 by Executive Order 13010, *Critical Infrastructure Protection*, which mandates that Government and industry cooperate to develop a strategy for protecting and ensuring continued National Information Infrastructure (NII) operation. The IPTF was assigned to focus its attention on the eight critical infrastructures: telecommunications, transportation, electric power, oil and gas (delivery and storage), banking and finance, water, emergency services, and continuity of Government services. Made up of twelve people from within the Federal Government and led by an FBI chairperson, the IPTF receives advice from a Steering Committee. The Steering Committee reports to a Principal's Committee, which reviews any reports or recommendations made to the President. Mr. McClurg serves as an FBI delegate to the IPTF alongside members from the National Security and Central Intelligence Agencies, National Communications System, and the Departments of Defense, Energy, Justice, Commerce, Transportation, and Treasury.

Executive Orders 12656, 12333, and the aforementioned 13010 assign responsibility to the FBI to coordinate the U.S. Government's criminal defense system, counter-intelligence and terrorism response system, and infrastructure protection responsibilities, respectively. These EOs and other statutes empower the FBI to conduct related investigations involving criminal, terrorist, and foreign power threats. Support, in the form of technology, personnel, or finances can be given to the FBI through the rest of the intelligence community, which includes the Department of Defense.

The FBI also retains jurisdiction in many cases through wording in combinations of documents. The Economic Espionage Act, for example, criminalizes some elements of

economically-related cyberwar, making this area of IW an area of FBI jurisdiction under Executive Order 12656. Cyberwar that can be traced to a foreign source can be deemed a matter of national security and thus is also under the jurisdiction of the FBI. Calling anything "foreign IW," however, is wishful thinking according to Mr. McClurg. It is unlikely that a purely foreign-based and foreign-operated threat would surface in light of all of the domestic opportunity for mischief. As for who should take charge of IW detection efforts at the national level, it is the opinion of Mr. McClurg that, in light of all of the legal documentation, which makes the FBI responsible for criminal investigations and foreign threats, the FBI should have been coordinating the effort to monitor cyberwar issues from the beginning. "Coordination is a natural precursor to protection," he asserts, "which is the basis for [the FBI-controlled area of] counter-terrorism."

To this end, in September 1996, Mr. McClurg was assigned as the Critical Infrastructure Protection Unit Chief in the FBI's Computer Investigation and Infrastructure Threat Assessment Center (CITAC). Originally called the Computer Investigation and Threat Assessment Center, this organization was expanded to address the issues of Critical Infrastructures after the issuance of EO 13010.

The CITAC Mission consists of the following:

- Program management of all computer intrusion investigations
- Technical/subject matter expertise in all other investigations involving computers
- Creation and maintenance of a "knowledge base"
- Production of infrastructure threat assessments
- Education and awareness outreach
- Coordination of efforts from the criminal investigative division and the national security division
- Identification of indications of foreign information warfare program capabilities, intention, and activities.

The CITAC, therefore, acts as a coordinating unit and bridges the gap between "domestic crime" investigations and the "foreign/national security" investigations for the purpose of investigating computer-related threats and crimes. Investigating these elements as a whole rather than separately is vital due to the fact that precursor events to a full IW/IO attack, which is a matter of national security, could appear as individual criminal acts in various locations. In McClurg's opinion, it is important to filter information to one place so the threat can be recognized as a true attack rather than as a series of unrelated

incidents. Mr. McClurg draws the parallel between the members of the CITAC and a SWAT team in that members of the CITAC tend to work on separate elements of a whole and come together for a common purpose just as the members of a SWAT team do.

The area of the CITAC responsible for comparison and analysis is the Watch and Threat Unit, parented at the current time by the Strategic Information and Operations Center (SIOP). The SIOP is a 24-hours-a-day, 7-days-a-week operation, making it an important resource for the Watch and Threat Unit, which has yet to attain 24/7 functioning. The SIOP and the Watch and Threat Unit of CITAC are designed to allow the FBI to "look at the big picture," for the purpose of detecting trends in cyber attacks and integrating information from many sources.

On a grander scale, there is cooperation between the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the FBI in looking at cyber threat. Weekly meetings between Computer Emergency Response Teams (CERTs) from each organization allow the groups to keep tabs on each other's investigations. DISA focuses its analyses on the Defense Information Infrastructure (the DII); the NSA focuses from a Federal Government perspective on the NII; and the FBI tends to bring in the NII information from the civil sector. The FBI has also been allowed to join the DoD CERT working group as its only non-military voting member, which allows the FBI more direct access to information gathered by the Department of Defense. Mr. McClurg views these partnerships as an opportunity to have a "virtual center" for IW between DISA, NSA, and the FBI. In this way, we could have Federal and civil criminal investigators sharing information about "suspect" IP addresses and a more thorough analysis could be done.

Proprietary information might be a problem in the civil sector, but this would be nothing with which the FBI has not dealt in the past. "You have to be able to filter information to one place so you can recognize threat as a true attack rather than isolated incidents."

It would help the monitoring situation, McClurg adds, if vendors in the information technology field would set defaults for security programs to "on" rather than "off." Many computers have monitoring devices or security programs in their makeup, but the default setting for these programs is usually "off," and, when companies are not making the effort to be aware of security, the default is usually not changed. The value of having the default set to "on," therefore, is that when the security is checked by the FBI or another

organization, data is available even though the company was not aware of or monitoring activity.

Other units of CITAC include the Special Technologies Applications Unit, the Strategic Planning and Analysis Unit, the Computer Investigations Unit, and the Critical Infrastructure Protection Unit (CIPU). The CIPU, headed by Mr. McClurg, acts as the liaison between the IPTF and the rest of the CITAC, conducts critical infrastructure research/analyses, provides training/education, and is tasked to issue national threat and warning notices and conduct after-action analyses.

In response to the question about coordination with our allies, Mr. McClurg suggested that our relations should remain the same as we delve into the cyberworld. American offensive planners must share information with American defensive planners because we can't assume that everyone else in the world is "behind" us in development of tactics and technology. Therefore, to defend ourselves we must know what we have to, or might have to, defend against. The defensive planners must confer amongst themselves between allies, however, in the face of a crisis. In some cases, this may compromise offensive planning information that one country would have liked to keep secret, but this is the risk run anytime countries ally themselves. It is not this kind of information leak that will be our problem; however, it is the problem of the human weak link. Mr. McClurg asserts that this problem of where to draw the line in the sharing of sensitive information will never be as big as the problem of the trusted insider who becomes an informant.

MELISSA MCPHERSON

RAND Corporation
July 1997

Question 1

IDA: What do you consider to be the major issues in the broad field of Information Operations, Information Warfare, Information Assurance?

MM: *If the question of major issues intentionally left room for interpretation, I'll address both of the angles that seem most obvious.*

Major issues as challenges:

- *Formulating a definition of information warfare, operations, assurance, etc., upon which all interested parties can agree*
- *Defeating skepticism and winning general acceptance of the relevance of the IW field*
- *Building consensus on what steps to take next*
- *Formulating national policy*
- *Establishing jurisdiction for the introduction and enforcement of new policies.*

Major issues as elements:

- *Information security (and therewith also information infrastructure assurance)*
- *War-making capacity*
- *Viable IW deterrence*
- *Social implications, that is, how will IW impact who makes war and what they want from war?*

Question 2

IDA: Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level? By the military? In the civil sector?

MM: *The military has made a good start on ensuring information security and building warmaking capacity, but they still have a long way to go. Deterrence has been largely ignored beyond the raising of the issue that it will be very difficult to establish; however,*

IW deterrence strategies will likely remain intractable until the U.S. experiences a true information war (which the Gulf War was not, by the way).

While White House initiatives have done much to increase awareness of information security needs, the civil sector's response has thus far been insufficient. Neither war-making capabilities nor deterrence really falls within the civil realm.

Social implications are the forgotten element, they have been ignored both by the military and by the civil sector. In writing, at least, the military has given almost no thought to the consequences of war's changes on society. A few writers in the civil sector have raised the issue, but most of them are viewed as sensationalist flag-wavers.

IDA: What do you see as challenges?

MM: *A common definition, acceptance of relevance, and consensus on next steps are all lacking in both the military and civil sector, though the former has spent a great deal more thought than the latter on trying to resolve these issues. White House initiatives on information infrastructure assurance are, again, crucial first steps, but there is still a great deal of policy backbone lacking. Also, it seems to me that very little of the impetus for policy has come from the military.*

Question 3

IDA: How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention?

MM: *I have no revolutionary suggestions, just the traditional litany of the academic: the solutions will require a fostering of greater general awareness and wider study. The difficulty with understanding the elements of information age conflict is that so much of what needs to be studied and brought to the public's attention has yet to happen, and much of it may not even happen at all, if predictions are wrong. The challenges of IW, however, might be more simply addressed by:*

- *Increasing simulation and modeling to build understanding of what information age war may be, how it may be fought, and how significant it is to conflict.*
- *Continuing national policy initiatives information assurance can, to a significant degree, be addressed even before we know what all the threats will be. However, policy needs to become increasingly coherent if it is to accomplish security objectives. Information security laws and regulations are vital here.*

Question 4

IDA: The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in the Government for dealing with this issue at the national level?

MM: *This, I'm sure you know, is a very tricky question. The paper I will be presenting at the September Infowar conference is a prelude for understanding why the roles of the military and domestic law enforcement are blurring. Confusion over the increasingly overlapping jurisdictions of military and law enforcement in the information age is a natural consequence of the fact that the civilianization of IW oversteps the established jurisdiction of warfare. (I'll attach the paper to give you a background for that statement.)*

As for prescriptions for dealing with this confusion, I think those closer to policy formulation would be better able to give recommendations; however, I know what I would not recommend.

I agree with the majority that it would be a mistake to make information warfare the sole jurisdiction of either the military or domestic law enforcement, especially before we have determined what part of the conflict spectrum (from peace, through peacekeeping, terrorism, and war) will present the most common threat (i.e., will it be more hacker crime or strategic warfare?).

Also, while centralized direction of information assurance is necessary, it would be dangerous to assume that one agency could take responsibility for every aspect of that defense. Rather, if an authoritative information agency is established, I would like to see it look more like what the CIA was intended to be. That is, an organization that directs a cooperating and integrated effort of a number of relevant agencies.

Question 5

IDA: What obstacles do you see to developing an effective national "cyber defense," and what should be done to overcome them?

MM: (1) *American culture, which values almost to the point of cultism the rights of privacy and freedom of speech,* (2) *the multiplicity of systems which need to be controlled and overseen for infrastructure assurance—more importantly, the multiplicity of actors*

(and interests) controlling them, (3) *also, the lack of incentive for investing in security: it's a cost outlay for a threat which most people do not yet believe will touch them.*

IDA: What is the answer to these obstacles?

MM: *Mandating legislation establishing security regulations, while at the same time ensuring that it is formulated to protect without smothering. That is, the legislation must not only take civil liberties into account, but obligation of the state to ensure the security of its people. To accompany this legislation and ensure its acceptance, the Government should also educate the public on the risks they face without that security.*

Question 6

IDA: How should the United States focus its resources to address the necessary elements of change and use these elements to its advantage as well as defend itself in the information age?

MM: *The key "value-added" of information technologies is that they increase capacity for efficient action. In warfare, this will manifest itself in the capability—and therefore, eventually, imperative—for decisive speed and accuracy.*

While critical infrastructure assurance is a vital first step, we need to turn to exploiting information technology's capacity for speed and precision on the battlefield for two reasons: (1) it could give us a decisive advantage, and (2) because if we do not develop this capability, our enemies eventually will develop it, and use it against us.

The military is already addressing this imperative for speed and accuracy in plans like Admiral Owens' system of systems and the development of Force XXI, but there is still considerable skepticism within the military and still a potential that they could go off track in their development of an information age military force.

To ensure that the military stays on track, they must emphasize the synergy of information—leveraging information technologies at the strategic, operational, and tactical, levels simultaneously to produce a decisive advantage and allow them to operate at a pace which opponents cannot match without comparable technology, organization, and planning.

Question 7

IDA: How should we approach the use of IW concepts and strategies with our allies to achieve an ordered response to crisis?

MM: *The United States faces large risks if its allies do not maintain a comparable level of information security and infrastructure assurance, especially if non-secure members become coalition partners in military actions. To counter this vulnerability, the U.S. should by all means share its advances in information security. However, strategy and weapon sharing should probably follow the same rules they do now, where sharing happens up to the point that it is in the U.S.'s interest of U.S. security and/or global stability.*

In this situation, the idea of vertical coalition assistance is particularly attractive: the United States provides the technology, a large portion of the intelligence (especially imagery and signals intelligence), and much of the know-how, while less IW-ready allies provide the manpower and the firepower.

This is a politically attractive policy because it would allow the U.S. to offer military assistance at little additional cost in American lives and treasure.

Question 8

IDA: What impact will the evolution of information technologies have on preventing and/or resolving conflicts with non-nation state actors (e.g., hackers, etc.)?

MM: *On the contrary, the primary impact of information warfare will not be that of preventing or resolving conflicts with non-state actors, but of making them more likely. Two trends in IW create a potential for non-state actors to compete viably in global strategic conflict for the first time in the history of the state system. These trends are the civilianization of IW, which, as it is relevant here, will allow non-state actors greater access to the tools of war; and the replacement of mass with efficiency as the decisive element in war. The efficiency/mass replacement reflects the rise of information power, which allows speed and precision to override benefits formerly accrued from mass in the industrial age cult of "bigger is better."*

Moreover, the rise of connectivity may actually encourage increased involvement in conflict. The Zapatistas in Chiapas, Mexico, are the most prominent example of a group and a struggle which would not have received world attention had it not been for the

Internet and other modern information technologies. One may also argue that the involvement of prominent, international non-governmental organizations in the Zapatistas' struggle actually mitigated the violence of the conflict. However, I believe that this mitigating effect will be outweighed by non-state actors' increased potential to compete in the global conflict arena.

Question 9

IDA: What prioritization of actions would you recommend? Where do we focus attention first and where do we go from there?

MM: *The United States must*

1. *Create a consensus on what information warfare (etc.) is. Without this agreement, all other IW initiatives may suffer. Creating a consensus may mean we agree to disagree—put a name on one phenomenon which deals primarily with information infrastructure attacks and assurance, and another name on the more military, strategic-level applications of information age conflict.*
2. *Determine what stands at greatest risk from IW and determine how to protect it, as well as who should do the protecting.*
3. *Develop and harden a minimum essential information infrastructure (MEII) as part of the protection of risk targets, and as a means of swift recovery from attack.*
4. *Determine where the risk may come from. Who has the potential to launch IW attack? (This is the project I am currently working on at RAND.) Who has the incentive to launch such an attack?*
5. *Continue development of our own capabilities for leveraging advantages in information technologies (this takes a relatively low position on the priority list partly because defense is more imperative, and partly because the U.S. has already done a great deal in this area and will not be caught totally by surprise at this point).*
6. *Before employing offensive IW (and, optimally, before defensive as well), the U.S. should examine the impact of war's changes on society and the international system and examine what these changes mean for the future use of war as an instrument of international politics.*

WINN SCHWARTAU

President of Interpact, Inc.
Madiera Beach, FL
January 2, 1998

Question 1

IDA: What do you consider to be the major issues in the broad field of Information Operations, Information Warfare, Information Assurance?

WS: *Number one, its a convergence issue: the needs and realities of the military and the needs of the civil sector are converging, and people who are trying to operate off in these little worlds of their own are really missing the whole point.*

Number two, a lot of people in the U.S. are trying to do it alone and it's not a problem in isolation—it's an international issue—and standing in isolation puts us standing in a Wilson-esque policy and we don't need that.

Thirdly, in the military there's a generational gap between the people who don't get it to the people who sorta get it to the people who really get it—and the people who really get it aren't in power yet.

IDA: With regard to the generational issue, can we do anything about it? Is it being addressed at all?

WS: *People in power don't give it up willingly, so the people who "get it," like some of the colonels and some of the baby birds, are really hamstrung in trying to do some of the far-reaching things they'd like to do. And this really affects policy because those who create policy are, by and large, the people who "don't get it." Sheehen made a great comment at Infowarcon a few years ago when he said that it's frightening to face the specter of a bunch of long-haired teenagers being able to take down portions of the military. There are some generals who really seem to get it, but there are certainly quite a few who don't. Many of them only see it in terms of battlefield dominance, and that's only a part of it.*

Question 2

IDA: Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level? By the military? In the civil sector?

WS: *I was hired by NATO to go in and brief them on these issues and I gave them a high-level briefing on the field...and to a man their jaws dropped. None of them know what this is about. Our congressmen don't know what this is about. The defense ministers I have met with, by and large, don't know what this is about. I think we need to step back and get our own house in order.*

And some of the major questions involved here are: What do we need to do? We don't have a policy. We don't have a vision. We don't have leadership in this country right now. We have administrative and legislative complacency that does not provide a national vision and without that we can't get our own house in order. And without our own house in order, how can we coordinate with other nations to deal with a global issue? And it is a global issue. But we can't deal with it as a global issue until we have some clue at home of what we want.

IDA: Whose responsibility is it to inform those who don't know?

WS: *Nobody's doing it.*

IDA: Who could?

WS: *Ultimately it has to come out of the White House. When Kennedy came out in the '60s and said, "we will land a man on the moon by the end of t he decade" that was a vision, that was a commitment, and it was bringing the nation together with a very single-pointed focus. When Churchill said at the end of WWII, "We will do anything necessary to save our land," that too was a focused statement. Nobody has come forward in our country to say that "we are going to do this, behave like this, here is America for the next 50 or 100 years." We don't have that kind of vision. We don't have that kind of single-pointed focus. We don't have stepping stones. And certainly one of them, from my perspective, is a redefinition of what we call national defense and national security. Though there are pockets of people who understand it, those people are not at the national policy level.*

IDA: Who should be telling those people who don't know? CIA? FBI?

WS: *The information is out there. That's one of the problems I had with the PCCIP. Let's go out and spend how many gazillions of dollars to find out that Schwartau's book was right and the Defense Science Board's study was right. Both of those said the same thing. I said it in 1994, and the DSB study said it in 1996. So they went out and spend a gazillion dollars to say, "Yeah, they're both right. The threat is probably even worse."*

The other thing that happened with the PCCIP was that it recommends total openness between the private sector and the Government. That's all talk and everything, but the report is classified! Talk about ironic misconfiguration of goal setting! That is awful. There are those fundamental problems but there is nothing new there. All it provided is a way to bludgeon more bureaucracy.

Question 3

IDA: How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention? Industry doesn't want to lose any money...how do we get them to communicate—and be honest?

WS: *That depends on what you're trying to accomplish. If you're talking about gathering statistics, let industry do what it has said that it is willing and wants to do. Anonymous reporting. All these characters in the Government are trying to say "No, no, no! You're going to give us the names, the dates, everything, so we can protect it." That's ridiculous! The biggest ones who let out secrets are the spies who are supposed to protect them. Let the private sector develop an anonymous reporting mechanism for whatever statistic databases you're trying to create, for whatever goal you're trying to achieve. We've been down that road. The second thing you've got to do is have an open source reporting mechanism that is coordinated and controlled—CERT-like but at more of an official level. But you can't do that until you have a policy response because, as of today, domestic law enforcement has legalized crime in this country. Now that crime is legal, all we're trying to do is allow law enforcement to grab credit for the high-profile crimes and to hell with the rest of them. So there's all this convoluted goals and policies and turf fightings and there is no national policy.*

IDA: What about the division between criminal and international acts? Do we need a whole new organization to deal with this threat?

WS: *We need a center of excellence. Based on a policy which is still not yet created. We do not know what war is. Does the DoD fit into this at all? The Secret Service is doing a good job of putting together the Electronic Crimes task force out in New York. The best FBI guy in the whole area just resigned: Chip Colgsworth. You've got Freeh up there trying to all this stuff—he is not long for the Bureau probably. And the CIA is still struggling to find a mission and the way to do it is to create a Center of Excellence and*

take the technical knowledge based upon some still as yet uncreated national policy and say, "Let's go." Defining the difference between terrorism and crime are huge problems.

Question 4

IDA: The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in the Government for dealing with this issue at the national level? Should we have some sort of center whether that be a physical structure or possibly networked?

WS: *You're not going to create virtual response, though, you need physical response. You can have virtual communication but you're going to have to have real bodies, real people. So you need a physical center to follow these things up. As far as CIA, FBI, etc., nobody knows who's in charge. Nobody is in charge. Especially since crime has become legal in the United States, which I maintain even though the FBI doesn't like hearing it, but when I lay out the facts for them, they admit it: they hate it. (But put it in your report, its all true.)*

The other thing that needs to be done at the very, very early level is that the Government has to be willing to declassify the threat. Part of the problem that you have is coordination between the private sector and the Government. And the Government is not trusted—just not trusted. You've got Cold War mind sets. Intelligence officers are the worst. The intelligence community seems to think they own the world of information. The military has (overall) been very open about these kinds of thing. Their classifications and secrets are with a wink and a nod and a napkin over a beer at an Arab restaurant in DC, and its amazing what you can find out. The Intel people though, they don't want the military involved, they don't want the private sector involved. But you have to have the private sector involved. They just like to think that all the stuff that's been in all the books that I've done and that everyone else has done is all secret! But we need to declassify the threat Once that happens, we can start having some of that openness that the PCCIP was talking about. But it's not going to happen overnight because of the immense amount of distrust.

IDA: With respect to the PCCIP, what would you have done differently?

WS: *Number one, I don't know one expert that they talked to. I'm not bragging, but I know a lot of people, and we were all talking trying to find out who the PCCIP talked to.*

Who was it? They talked to upper-level management in infrastructure areas that do not get it. They don't know how to handle this stuff. They did not talk to the right people.

Number two, it was a total rehash of things that have been done before. There was nothing new, nothing novel, and it didn't contribute a damned thing. All it said was, "Yeah, we've got a problem. All the things that have been done before are right. Let's go create a bureaucracy." I think that, to a large extent, this is a whitewash. The commission was charged never to use the word "cryptography" and cryptography is the foundation of any defensive mechanisms at any level, yet they're charged not to because it is politically derailing because the truth of cryptography is the antithesis of what the Government has been trying to do. So, I'm not a big fan of the results of the PCCIP.

Question 5

IDA: What obstacles do you see to developing an effective national "cyber defense," and what should be done to overcome them?

WS: [I outlined an approach] *in my book but Electronic Civil Defense* [which called for] *a convergence between law enforcement and military defense based on new national security realities, and we've not done any of that yet. Reclassification of what is classified in the military sector is crucial. For example, we enter into an operation—a conventional operation with real soldiers going to a real place. Regardless of what the mission is, the military classifies certain aspects of that mission—goals, names, all those kinds of good stuff for the forward-deployed troops and operations. The rear-echelon support mechanism, which occurs across private, domestic, commercial infrastructure is all unclassified. Would I go after the soldier who's got thirteen satellites and a billion howitzers? No, I'm going to go after the toilet paper supplies, the food supplies; I'm going to go after the commercial, unclassified, rear-echelon support mechanisms. I talked to Sheehen* [former CINCLANT] *about this and he agreed that a redefinition of what is in the circle of classification for certain types of operations is in order because right now we classify only a small piece of the mission and the whole support mechanism is unclassified. Something's wrong here.*

The issue of social change and the structure of social change has to be reanalyzed. I've done a number of reports on the distinctions between two-dimensional societies and three-dimensional societies, and we're trying to converge the two in terms of function. How do we survive and move forward in global economies and how do we battle between a two-

dimensional adversary and a three-dimensional good guy? Three-dimensional good guy: the Pentagon, which is a heirarchal management-oriented. Three-dimensional structure: IBM, General Motors, any "second-wave" Tofflerist kind of organization. The Internet and terrorist organizations are flat, they're cell-based. Pockets of things, all of them co-equal with regard to the topology of that particular piece of society with ripples of leadership that appear periodically and then ripple back down for another one to ripple up later. This is the exact model of terrorist organizations worldwide, and we've not figured out how to battle them yet! So we have a sociological issue here that has to be dealt with as well, and that is the convergence of the two- and three-dimensional societies.

Question 6

IDA: How should the United States focus its resources to address the necessary elements of change and use these elements to its advantage as well as defend itself in the information age?

WS: *We need to build up a kind of a graceful degradation in the network society. Bad guys may or may not be coming—immaterial. We dealt with the Cold War with Electronic Civil Defense. That concept needs to be fast-forwarded to today. Our vulnerability is not going to be the missiles coming in at all. It's going to be the systemic collapse of portions of critical infrastructure. Therefore, how do we defend ourselves against that? So we can get into all the technical aspects at the front line of defense, but from a protective mechanism farther down the line we need to design graceful degradation systems to be able to absorb a hit. How can we design "absorbing a hit" in the airline industry, the power industry? How can Florida survive if Georgia is taken out? How do all these things interconnect at a network basis? We can do it on certain types of networks and distributed systems. The Internet, for example, was designed to do this. Nowadays it sort of works, but we need to extend this same type of survivability model and apply it to the national economic critical infrastructure systems.*

Question 7

IDA: How should we approach the use of IW concepts and strategies with our allies to achieve an ordered response to crisis?

WS: *We can't work with our allies until our own house is in order. This is an international issue, and we must be able to work freely with our allies.* [Earlier comments in Question 2 about working with NATO.]

Question 8

IDA: What impact will the evolution of information technologies have on preventing and/or resolving conflicts with non-nation state actors (e.g., hackers, etc.)?

WS: *Non-nation state actors...this one goes back to the two-dimensional structure of the planet. They're now equal! When we get into all these curves and stuff that I've done, they show the flattening of the bipolar militaristic world to the unipolar militaristic world. Non-nation state actors create a lot more problems, therefore, partly because of their equality and also partly because of the lack of being able to respond in a conventional three-dimensional manner in a two-dimensional conflict. So, in a non-physical conflict you've effectively raised them to the same level as everyone else.*

Question 9

IDA: What prioritization of actions would you recommend? Where do we focus attention first and where do we go from there?

WS: *My suggested prioritization of actions would be to focus on the following items:*

- *Build a national leadership for the subject*
- *Create a Center of Excellence for study and analyses*
- *Declassify the threat and allow Government and industry to work together*
- *Reconsider the area of classification within military operations, especially support mechanisms.*

(This page is intentionally blank.)

HOWARD WHETZEL

President, Avenue Technologies, Inc.
Former Assistant to the Director, DIA for Electronic Warfare and Joint C3I Systems
July 14, 1997

Question 1

IDA: What do you consider to be the major issues in the broad field of Information Operations, Information Warfare, Information Assurance?

HW: *Information Warfare is a strategy, not a breakdown of programs. It is similar to command, control and communications countermeasures (C3CM), long defined as a basic strategy integrating several warfighting functions into one coherent whole.*

Outside of war on land and war in the air, there was always "war in the ether," which refers to other elements of war besides physical destruction. This "war in the ether" has morphed into a more concrete form, which we define as "war in cyberspace."

The major aspects of this new capability is a proper task for the intelligence community, and they should be focusing on solutions and options.

Question 2

IDA: Do you feel that these issues are currently being sufficiently addressed at both a national and a Department of Defense level? By the military? In the civil sector?

HW: *With respect to the military, there is a generational gap between those in command and those who are out in the field working with technology. People in charge do not understand the impact that technology is having. There is some understanding of vulnerability but little understanding of scope.*

In the civilian world, there is little thought given to these issues. Without the now universally touted "electronic Pearl Harbor" there will likely be no action taken. Security and foresight will mean money, and the American mindset is, "when I have to spend money I will."

Questions 3 & 4

IDA: How would you propose to address any issues, on the offensive IW front and/or the defensive IA side, which you believe are not yet receiving attention?

The evolution of information technologies affects the traditional roles and boundaries of responsibilities both within the DoD and at the national level. Who do you feel has the underlying responsibility in the Government for dealing with this issue at the national level?

HW: *One of our greatest weakness is that we have no national center to deal with issues pertaining to InfoWar. A number of our potential adversaries have centers, but we have neither a center nor a national strategy for the purpose of InfoWar defense or offense. As far as the creation of a center is concerned, the Government doesn't want to create one because it would force them to create a new bureaucracy. Until we have some sort of "electronic Pearl Harbor" we probably will not go in that direction.*

We can *keep adding responsibility to existing bureaucracies like the FBI/CIA/DoD. This will enlarge those existing bureaucracies, but it will avoid the addition of a new one. Congress could find the extra money to do this, but no one has come up with a strategic plan. Division of responsibilities should be handled in the obvious way: the DoD and CIA should deal with security of the U.S. against actions by foreign powers; and the FBI should provide internal U.S. support, protection, and prosecution of domestic offenders (e.g., criminals, terrorists, disgruntled insiders). Within the CIA, there should be a cooperative arrangement with NSA and the DIA for sharing information and providing warnings of attack; the DIA should also act as a database center. The FBI's role would continue to be dealing with criminal investigations and prosecutions within the U.S. The President is the only one who could mandate this kind of inter-agency cooperation, but as yet this has not happened.*

Question 6

IDA: How should the United States focus its resources to address the necessary elements of change and use these elements to its advantage as well as defend itself in the information age?

HW: *The President's Commission on Critical Infrastructure Protection (PCCIP) should have emphasized the need for people from Government agencies, not the civil sector. We must look to the Government first to set the example rather than the civil sector. Reorganization of Government responsibilities with specific assignments and authorities would serve as a model for the rest of the private sectors and country to follow.*

Question 7

IDA: How should we approach the use of IW concepts and strategies with our allies to achieve an ordered response to crisis?

HW: *Most of our allies don't have the same problems we do since they're not at the same point of development in the IW field as we are. The Canadians, the Brits, the Germans—none of them have encountered the same problems with the developing technologies, so they haven't responded the same way in crisis situations.*

Question 9

IDA: What prioritization of actions would you recommend? Where do we focus attention first and where do we go from there?

HW:

- *Must allocate responsibilities of who is in charge.*
- *Create an organization which centralizes who's in charge of actions taken.*
- *Need designation of some responsibilities to current bureaucracies. We do need contractor or Government manpower and money, but that is* all *we need from them.*
- *The baseline is this: If you have no group or individual who is in charge of monitoring possible IW activity, you will not even know you are being attacked.*

(This page is intentionally blank.)

Appendix C

ACRONYMS

Appendix C
ACRONYMS

ADP	automated data processing
AFCEA	Armed Forces Communications & Electronics Association
AIP	AFCEA International Press
ANSIR	Awareness of National Security Issues and Response
C2	command and control
C2W	command and control warfare
C3	command, control, and communications
C3I	command, control, communications, and intelligence
C3CM	command, control, and communications countermeasures
C4	command, control, communications, and computers
C4ISR	command, control, communications, computers, intelligence, surveillance, and reconnaissance
CBAT	Campaign Builder and Analysis Tool
CCU	Computer Crime Unit
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CINCLANT	Commander in Chief, Atlantic
CIPU	Critical Infrastructure Protection Unit
CITAC	Computer Investigation and Infrastructure Threat Assessment Center (FBI)
CJCS	Chief, Joint Chiefs of Staff
CNN	Cable News Network
COMPUSEC	computer systems security
COMSEC	communications security
COTS	commercial off-the-shelf
DARPA	Defense Advanced Research Projects Agency

DEW	Defense Early Warning System
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIS	Defense Investigative Service
DISA	Defense Information Systems Agency
DMA	Defense Mapping Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDII	Department of Defense Information Infrastructure
DSB	Defense Science Board
ECCM	electronic counter-countermeasures
EO	Executive Order
EW	electronic warfare
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FPGA	field programmable gate arrays
GAO	Government Accounting Office
GCCS	Global Command and Control System
GSA	General Services Administration
IA	Information Assurance
IATF	Information Assurance Task Force
IBW	Intelligence-Based Warfare
INFOSEC	information systems security
INFOWARCON	Information War Conference
IO	Information Operations
IPTF	Infrastructure Protection Task Force
I-TRAP	Interagency Terrorism Response Awareness Program
IW	Information Warfare
IW-D	Information Warfare–Defense
IW-O	Information Warfare–Offense

JCS	Joint Chiefs of Staff
JP	Joint Publication
JPI	Joint Precision Interdiction
JV 2010	Joint Vision 2010
MISSI	multilevel information systems security initiative
MOP	Memorandum of Policy
NCS	National Communications System
NDU	National Defense University
NII	National Information Infrastructure
NPS	Naval Post-Graduate School
NRC	Nuclear Regulatory Commission
NRO	National Reconnaissance Office
NSA	National Security Agency
NSD	National Security Directive
NSTAC	National Security Telecommunications Advisory Committee
NSTISSC	National Security Telecommunications and Information Systems Security Committee
OMB	Office of Management & Budget
OSD	Office of the Secretary of Defense
PCCIP	President's Commission on Critical Infrastructure Protection
PSYOPS	psychological operations
QDR	Quadrennial Defense Review
R&D	research and development
RADM	Rear Admiral
REC	radio electronic combat
SOLIC	Special Operations–Low Intensity Conflict
STRATCOM	Strategic Command

USAF	U.S. Air Force
USN	U.S. Navy
WMD	weapons of mass destruction
WWII	World War II

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1997	Final

4. TITLE AND SUBTITLE

Information Operations: A Research Aid
Includes Coverage of: Information Warfare, Information Assurance, Infrastructure Protection

5. FUNDING NUMBERS

DASW01-94-C-0054

CRP 9001-134

6. AUTHOR(S)

William J. Barlow, John W. Barnett, John L. Gerrity, Jaime V. Gray, Robert D. Turner

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Institute for Defense Analyses
1801 N. Beauregard Street
Alexandria, VA 22311-1772

8. PERFORMING ORGANIZATION REPORT NUMBER

IDA Document D-2082

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The purpose of this paper is to provide an aid for researchers engaged in studying aspects of military Information Operations; IO includes subelements of Information Warfare, Information Superiority, and Information Assurance. These topics are also associated with National Critical Infrastructure Protection. The document sets forth an annotated bibliography of research material arranged by principal subject areas (e.g., Information Operations, Defensive Information Operations, National Policy, Technology) believed to be of most value to new analysts of this field. Also included are the results of interviews conducted with several nationally recognized experts in an attempt to elicit main themes and suggestions for improvement. In view of the explosion of new terms, concepts, and taxonomies in the information field, this document is believed to provide an excellent starting point for identifying issues and options, as well as applicable policy and implementation publications.

14. SUBJECT TERMS

Information Warfare, Information Assurance, Infrastructure Protection, Information Operations, Information Systems Security, Computer Systems Security, National Information Infrastructure, Defense Information Infrastructure

15. NUMBER OF PAGES

127

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	Unlimited